UNIVERSIDAD INTERNACIONAL DE LA RIOJA

**Universidad Internacional de La Rioja**
**Máster universitario en Seguridad Informática**

# Gestión del riesgo con base en ISO27005 adaptando OCTAVE-S

**Trabajo Fin de Máster**

**presentado por:** Amador Donado, Siler

**Director/a:** Martínez Herraíz, José Javier

Ciudad: Popayán, Colombia
Fecha: 14 de Diciembre de 2014

Siler Amador Donado
D.N.I 72.168.640

# Tabla de contenido

Siler Amador Donado
D.N.I 72.168.640

Siler Amador Donado
D.N.I 72.168.640

**Resumen**

Este documento presenta la aplicación de la metodología OCTAVE-S para el análisis y gestión del riesgo en la seguridad de la información, adaptada al *caso de estudio*[1]. El objetivo general es **gestionar el riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S al *caso de estudio*.** Además se incluye la estructura del proceso y el procedimiento escogido como caso de estudio para aplicar el tratamiento del riesgo. Finalmente, se muestran los resultados obtenidos y las conclusiones de la gestión del riesgo con la metodología adaptada.

**Palabras Clave:** Gestión del riesgo, SGSI, Riesgo de seguridad de la información, amenaza, impacto, ISO/IEC 27005, Metodología de las Elipses, Metodología OCTAVE-S.

**Abstract**

This paper presents the application of OCTAVE-S methodology for the analysis and management of risk in information security adapted to the process Registration and Admissions, Division of Registration and Academic Admission Control (DARCA) at the University of Cauca; following the directives of ISO / IEC 27005: 2011. The overall objective is **to manage risk in information security based on ISO / IEC Standard 27005, 2011, proposing an adaptation of the OCTAVE-S methodology to the *case study***. Also the structure of the process is included, and the method chosen as a case study to implement risk treatment. Finally, the results and conclusions of the risk management methodology is adapted.

**Keywords:** Risk management, ISMS, Risk information security, threat, impact, ISO/IEC 27005, Ellipses Methodology, Methodology OCTAVE-S.

**Resumen de la estructura del documento en capítulos**

[1] Proceso Inscripciones y Admisiones de DARCA (División de Admisión Registro y Control Académico) de la Universidad del Cauca; siguiendo las directrices de la norma ISO/IEC 27005:2011

**Capítulo 1**: Se realiza una *introducción* a la temática teniendo en cuenta el *contexto*, luego se aborda el *planteamiento del problema* y finalmente se establecen los objetivos generales y específicos.

**Capítulo 2:** Se realiza el *marco teórico* de la temática y luego se aborda el *estado del arte* de la gestión, implantación y metodologías de análisis de riesgo.

**Capítulo 3**: Se realiza el diseño del diagrama de flujo de información del proceso de inscripciones y admisiones, luego se aborda la definición del calendario, justificación del servicio, inscripciones, alistamiento, aplicación y evaluación de la prueba y admisiones.

**Capítulo 4:** Se realiza un desarrollo en profundidad de las 3 fases de la metodología de análisis y gestión del riesgo OCTAVE-S.

**Capítulo 5:** Se realiza un contraste de las 3 fases de la metodología de análisis y gestión del riesgo OCTAVE-S y la Norma ISO 27005.

**Capítulo 6:** Se realizan las conclusiones, beneficios, recomendaciones y se proponen trabajos futuros.

Siler Amador Donado
D.N.I 72.168.640

# 1 Introducción

## 1.1 Contexto

En la actualidad, las empresas manejan la información referente a sus procesos de negocio de forma física y digital. Dicha información, independiente de su medio de almacenamiento y transmisión, es un recurso vital para el éxito y la continuidad del servicio en cualquier organización, ya que de ella depende la toma de decisiones y el conocimiento interno de la empresa.

Debe tenerse en cuenta que un sistema de información no necesariamente está asociado a un sistema informático. Un sistema de información pueden ser personas, materiales, objetivos, actividades, etc., aunque también tecnologías de la información y de comunicación. Es por esto que la gestión del riesgo en la seguridad de la información debe considerar aspectos tanto físicos como lógicos para lograr un adecuado tratamiento del riesgo.

La gestión del riesgo en la seguridad de la información implica inversión de tiempo, esfuerzo y otros recursos con los que una pequeña organización no suele disponer, siendo esta una de las razones por las que no suelen ejecutar La gestión del riesgo como una prioridad.

Las organizaciones que conocen el valor de sus activos de información y desean invertir en gestionar su riesgo, suelen acogerse a las normas de la familia ISO 27000, en especial la norma ISO 27005. **Dicha norma contiene las directrices que se deben realizar para llevar a cabo el proceso de gestión del riesgo, pero no cómo se debe realizar; es por esto que se hace necesario definir y seguir una metodología que se adapte al entorno o contexto a abarcar**, es aquí donde una organización toma la decisión más importante en el proceso de gestión del riesgo, ya que elegir la metodología inadecuada traerá como resultado ineficiencia y por lo tanto mayor costo y esfuerzo para lograr el objetivo, que consiste en administrar el riesgo de manera eficiente y económica de lo que costaría recuperarse de un incidente de seguridad.

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones del negocio, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, etcétera y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

Cada organización tiene una misión y visión y para llevarlas a cabo, las organizaciones utilizan las TIC para automatizar sus procesos o información y deben tener en cuenta que la gestión del riesgo informático es muy importante para la optimización de sus procesos y procedimientos administrativos.

Uno de los objetivos principales de la administración del riesgo de la información debe ser "procurar que la organización logre llevar a cabo su misión" no solamente proteger sus activos de información. El riesgo es la forma en que impacta negativamente una vulnerabilidad, considerando su probabilidad y la importancia de ocurrencia. Por lo que fácilmente podemos deducir que la gestión de riesgos es un proceso cíclico de identificación, evaluación y toma de decisiones que busca reducir el riesgo a un nivel aceptable.
Por todo esto se vuelve indispensable que la metodología de análisis de riesgos que se escoja cumpla las necesidades de la organización y se logre adaptar a sus limitaciones.
Teniendo en cuenta las consideraciones mencionadas anteriormente, este documento aborda una propuesta del cómo llevar a cabo la gestión del riesgo en la seguridad de la información según la norma ISO/IEC 27005:2011, proponiendo una adaptación de la metodología OCTAVE-S para ser aplicada al *caso de estudio*, con el fin de minimizar el riesgo actual de dicho proceso.

### 1.2 Planteamiento del Problema

Al estudiarse las metodologías de análisis de riesgos de seguridad de la información existentes por parte de la organización, surge la duda de cuál de todas es la adecuada y que se pueda aplicar fácilmente a los procesos y procedimientos de la organización. Las organizaciones en su mayoría como la de nuestro *caso de estudio*, no conocen el valor de sus activos de información y mucho menos de los riesgos de seguridad de la información a los que se enfrentan diariamente. Esto es debido a que no llevan a cabo una gestión adecuada del riesgo, es decir no se realizan actividades de manera periódica como:

1. Identificar las amenazas
2. Identificar las vulnerabilidades
3. Revisar los controles actuales
4. Calcular el nivel de exposición al riesgo
5. Determinar escenarios de amenazas

Los riesgos pueden existir tanto en el exterior como en el interior de la organización, atentando contra la seguridad de los activos de información de la misma; por ello, se ve la necesidad de analizarlos, evaluarlos y tratarlos adecuadamente. Es ahí donde las normas ISO/IEC (International Organization for Standarization / International Electrotechnical Commission) 27001:2005, 27002:2005 y 27005:2011, sirven de modelo para conocer y gestionar el riesgo mediante la implantación de un SGSI[2].

[2] Sistema de Gestión de la Seguridad de la Información

En cuanto a la necesidad de gestión de riesgos de los activos de información del *caso de estudio*, se identifica la necesidad de implantar un SGSI, que está enmarcado dentro del proyecto llamado: "**Implantación y certificación del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad del Cauca**", teniendo en cuenta la norma ISO/IEC 27001:2005 [1], del cual se han desarrollado dos proyectos más, a saber: "*Sistema de alertas de seguridad informática para los servicios críticos de la división de tecnologías de la información y la comunicación*", y "*Controles inteligentes sobre el SGSI*[3]", con el propósito de llegar a la implantación, certificación y desarrollar un SGSI.

Para el desarrollo del SGSI se requiere llevar a cabo la etapa **PLAN** del *ciclo Deming* la gestión del riesgo de la información; para esto, la organización debe tener en cuenta los procesos críticos, con el objetivo de gestionar la seguridad de los activos de información a través de su evaluación, tratamiento y aceptación del riesgo, considerando la **confidencialidad**, **integridad** y **disponibilidad**.

El proceso crítico tomado como caso de estudio en este TFM es "Inscripciones y Admisiones" de la División de Admisiones, Registro y Control Académico (DARCA), en el cual se gestionará el riesgo, aplicando como modelo la norma ISO/IEC 27005 de 2011 [2]. Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un SGSI de acuerdo con la norma ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. **Corresponde a la organización definir su metodología para la gestión del riesgo**, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial.

Por lo tanto, se hizo necesario examinar las metodologías de análisis y gestión de riesgos de mayor importancia y aceptación a nivel mundial, siguiendo los estudios y recomendaciones presentes en los documentos [10], [11], [21], [24]; llegando a la conclusión que la metodología OCTAVE-S es la que mejor se acopla al caso de estudio del TFM.

De lo anterior surge la siguiente pregunta:

¿Es posible adaptar la metodología OCTAVE-S al caso de estudio, para la gestión del riesgo en la seguridad de la información, cumpliendo las directrices de la norma ISO/IEC 27005 de 2011?

[3] http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XIII_JornadaSeguridad/Articulo2DesarrollodecontrolesparaelSGSI_Unicaucaaplicandotecnicasdeinteligenciaartificial.pdf

## 1.3 Objetivos

### 1.3.1 Objetivo general

Gestionar el riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S al *caso de estudio*.

### 1.3.2 Objetivos específicos

1. Definir el alcance del caso de estudio aplicando la Metodología de las Elipses[4] al Proceso de Inscripciones y Admisiones en DARCA e identificar los subprocesos y dependencias con otros procesos de la Universidad del Cauca y su interacción con entidades externas.
2. Adaptar la metodología de análisis y gestión del riesgo OCTAVE-S al *caso de estudio* cumpliendo con las directrices de la norma ISO/IEC 27005.
3. Efectuar la gestión del riesgo al *caso de estudio* con base en la adaptación de la metodología de análisis y gestión del riesgo OCTAVE-S.

### 1.3.3 Metodología para el cumplimiento de los objetivos

En el diagrama de flujo se describe los pasos realizados para el cumplimiento de los objetivos planteados para el desarrollo de este TFM. El diagrama se encuentra en el Anexo A.

[4] Es un método que permite identificar los distintos tipos de activos de información existentes dentro del alcance del modelo.

Siler Amador Donado
D.N.I 72.168.640

# 2 Marco teórico y estado del arte

## 2.1 Marco Teórico

### 2.1.1 Impacto

El efecto de una amenaza sobre la misión de la organización y los objetivos de negocio.

### 2.1.2 Valor de impacto

Una medida cualitativa del impacto de un riesgo específico para la organización (alta, media o baja).

### 2.1.3 Criterios de evaluación de impacto

Un conjunto de medidas cualitativas contra el cual se evalúa el efecto de cada riesgo en la misión de la organización y los objetivos de negocio. Criterios de evaluación de impacto definen rangos de impacto alto, medio y bajo para una organización.

### 2.1.4 Activos

Algo de valor para la empresa. Activos de tecnología de la información son la combinación de los activos físicos y lógicos y se agrupan en clases específicas (información, sistemas, servicios y aplicaciones, personas).
Categorías de activos:

1. Información: documentado (en papel o electrónicos) de datos o la propiedad intelectual utilizada para cumplir con la misión de una organización.
2. Sistemas: una combinación de la información, el software y los activos de hardware que procesan y almacenan información. Cualquier servidor, cliente o servidor puede ser considerado un sistema.
3. Servicios y aplicaciones: aplicaciones y servicios de software (sistemas operativos, aplicaciones de bases de datos, software de red, aplicaciones de oficina, aplicaciones a medida, etc.) que procesan, almacenan o transmiten información.
4. Personas: las personas en una organización y que poseen habilidades únicas, el conocimiento y la experiencia que son difíciles de reemplazar.

### 2.1.5 Prácticas de seguridad

Acciones que ayudan a iniciar, implementar y mantener la seguridad dentro de una empresa.

### 2.1.6 Vulnerabilidades organizacionales

Debilidades en la política o en la práctica organizacional que pueden resultar en acciones no autorizadas.

### 2.1.7 Catálogo de prácticas

Una colección de buenas prácticas estratégicas y operativas de seguridad que una organización puede utilizar para gestionar su seguridad.

### 2.1.8 Prácticas estratégicas

Prácticas de seguridad que se centran en cuestiones de organización a nivel de políticas. Estos incluyen problemas relacionados con la empresa, así como cuestiones que requieren los planes y la participación de toda la organización.

### 2.1.9 Prácticas operacionales

Prácticas de seguridad que se centran en cuestiones relacionadas con la tecnología. Estos incluyen problemas relacionados con la forma en la gente usa, interactuar con, y proteger la tecnología sobre una base del día a día.

### 2.1.10 Estado de la luz de parada

Lo bien que una organización está llevando a cabo en un área de práctica de seguridad. Los siguientes colores son asignados a un área basada en el rendimiento percibido en esa zona:

1. Verde: La organización está llevando a cabo las prácticas de seguridad en el área muy bien; no hay necesidad real para la mejora.
2. Amarillo: La organización está llevando a cabo las prácticas de seguridad en cierta medida; hay espacio para la mejora.
3. Rojo: La organización no está realizando las prácticas de seguridad en la zona; existe un amplio margen de mejora.

### 2.1.11 Activos críticos

De los activos más importantes para una organización. La organización va a sufrir un gran impacto negativo si:

1. Un activo crítico se da a conocer a las personas no autorizadas
2. Un activo crítico es modificado sin autorización
3. Un activo crítico se pierde o destruye
4. Acceso a un activo crítico se interrumpe

### 2.1.12 Requisitos de seguridad

Declaraciones que describen las cualidades de los activos relacionados con la información que son importantes para una organización. Requisitos de seguridad típicas son la confidencialidad, integridad y disponibilidad.

### 2.1.13 Confidencialidad

La necesidad de mantener información confidencial, sensible o personal privado e inaccesible a cualquier persona que no esté autorizada a verlo.

### 2.1.14 Integridad

La autenticidad, precisión y exhaustividad de un activo.

### 2.1.15 Disponibilidad

Cuándo o con qué frecuencia debe estar presente o lista para su uso de un activo.

### 2.1.16 Amenaza

Una indicación de un posible evento indeseable. Una amenaza se refiere a una situación en la que una persona puede hacer algo indeseable (un atacante inicia un ataque de denegación de servicio contra el servidor de correo electrónico de una organización) o un fenómeno natural podría causar un resultado no deseado (un incendio que altere la información del hardware de tecnología de la organización).
Las amenazas se representan mediante las siguientes propiedades:

1. Activos - algo de valor para la empresa.
2. El acceso - cómo se accede al mismo por un actor (acceso a la red, el acceso físico). El acceso sólo se aplica a los actores humanos.
3. Actor - quién o qué puede violar los requisitos de seguridad (confidencialidad, integridad, disponibilidad) de un activo
4. Motivo - la intención del actor (por ejemplo, deliberada o accidental). Motivo se aplica sólo a los actores humanos.
5. Resultado - el resultado inmediato (divulgación, modificación, destrucción, pérdida, interrupción) de violar los requisitos de seguridad de un activo.

### 2.1.17 Perfil Amenaza

Una forma estructurada de la presentación de una serie de amenazas a un activo crítico. Amenazas en el perfil se agrupan de acuerdo a la fuente de la amenaza.

### 2.1.18 Perfil genérico amenaza

Un catálogo de amenazas que contiene una variedad de todas las posibles amenazas que se consideran. El perfil genérico amenaza es un punto de partida para crear un perfil de amenaza única para cada activo crítico.

### 2.1.19 Las rutas de acceso de red

Formas en que los sistemas, dispositivos, información o servicios se pueden acceder a través de la red de una organización.

### 2.1.20 Sistema De Intereses

El sistema o sistemas que están más estrechamente ligada a un activo crítico, por ejemplo:

1. El sistema en el que el activo "reside"
2. El sistema donde va a ir para obtener una copia "oficial" del activo

3. El sistema que ofrece a los usuarios legítimos el acceso a un activo crítico
4. El sistema que le da un acceso al actor de amenaza a un activo crítico

#### 2.1.21 Clases principales de componentes

Categorías de dispositivos y redes que se utilizan para acceder a un sistema de interés. Estos dispositivos y redes son parte de o en relación con un sistema de interés. Cuando los usuarios legítimos accedan a un activo crítico, acceden a componentes de esas clases. Actores de amenazas también acceden a componentes de esas clases cuando los actores se dirigen deliberadamente a un activo crítico.

#### 2.1.22 Los puntos de acceso

Interfaces que, directa o indirectamente, permiten el acceso a un sistema de interés. Estas interfaces se agrupan de acuerdo a las siguientes categorías:

1. Los componentes del sistema de interés
2. El acceso al sistema por personas
3. Puntos de acceso intermedio
4. Otras interfaces y los lugares de almacenamiento de datos
5. Otros sistemas

#### 2.1.23 Acceso al sistema por la gente

Los tipos de componentes que la gente (por ejemplo, los usuarios, los atacantes) utilizan para acceder a un sistema de interés. Estos componentes constituyen los puntos de acceso que pueden originar internamente o externamente a los sistemas y redes de una organización.

#### 2.1.24 Puntos de acceso Intermedio

Redes que se utilizan para transmitir información y las aplicaciones del sistema de interés para las personas.

#### 2.1.25 Lugares de almacenamiento de datos

Otros tipos de componentes que se utilizan para almacenar información crítica o proporcionar servicios de apoyo a los datos relacionados con un sistema de interés (por ejemplo, dispositivos de almacenamiento utilizados para respaldar la información almacenada en un sistema de interés).

#### 2.1.26 Riesgo

La posibilidad de sufrir daños o pérdidas. El riesgo se refiere a una situación en la que una persona puede hacer algo indeseable o un fenómeno natural podría causar un resultado indeseable, lo que resulta en un impacto negativo o consecuencia. Un riesgo se compone de:

- Un evento
- Una Incertidumbre
- Una consecuencia

En seguridad de la información, el evento básico es una amenaza.
La incertidumbre se manifiesta en gran parte de la información recopilada durante la evaluación OCTAVE-S. Hay incertidumbre en torno a si se producirá una amenaza y si la organización está suficientemente protegido contra el actor amenaza. La incertidumbre se representa a menudo usando la probabilidad de ocurrencia o probabilidad.
La consecuencia que importa en última instancia en el riesgo de seguridad de la información es el impacto resultante en la organización debido a una amenaza. Impacto describe cómo una organización puede verse afectada según los siguientes resultados de amenaza:

- Divulgación de un activo crítico
- Modificación de un activo crítico
- Pérdida / destrucción de un activo crítico
- Interrupción de un activo crítico

Los resultados mencionados anteriormente están directamente relacionados con los activos; ellos describen el efecto de las amenazas sobre los activos. El impacto se centra en la organización; es el enlace directo a la misión y los objetivos de negocio de la organización.

#### 2.1.27 Probabilidad

Es un método por el cual se obtiene la frecuencia de un acontecimiento determinado.

#### 2.1.28 Valor de probabilidad

Es la frecuencia medida de forma cualitativa (alta, media o baja) y cuantitativa (3, 2, 1) del aprovechamiento de la vulnerabilidad por parte de la amenaza.

#### 2.1.29 Criterios de evaluación de la probabilidad

Un conjunto de medidas cualitativas utilizadas para estimar la probabilidad de ocurrencia de una amenaza. Los Criterios de evaluación de la probabilidad

definen los rangos de frecuencia de alta, media y baja probabilidad; indican con qué frecuencia se producen amenazas durante un período de tiempo común.

### 2.1.30 El tiempo entre eventos

Una estimación de qué tan frecuente podría ocurrir un evento (por ejemplo, cada semana, una vez cada dos años).

### 2.1.31 Frecuencia anualizada

La probabilidad proyectada de ocurrencia de una amenaza en un año determinado.
En OCTAVE-S, los valores de probabilidad se definen por un conjunto de criterios de evaluación que se clasifican de acuerdo a la frecuencia de ocurrencia. Los criterios de evaluación de probabilidad definen un conjunto estándar de definiciones de valores de probabilidad. Estos criterios definen las medidas de alto, medio y bajo de probabilidades de amenaza.
Las medidas de probabilidad se definen teniendo en cuenta un rango de frecuencias (es decir, la probabilidad de ocurrencia de una amenaza en un año determinado):

- Diario
- Semanal
- Mensual
- 4 veces al año
- 2 veces al año
- Una vez al año
- Una vez cada 2 años
- Una vez cada 5 años
- Una vez cada 10 años
- Una vez cada 20 años
- Una vez cada 50 años

Un riesgo se compone de:

- Un evento
- Incertidumbre
- Una consecuencia

La incertidumbre se manifiesta en gran parte de la información recopilada durante la evaluación. Hay incertidumbre en torno a si se producirá una amenaza y si la organización está suficientemente protegido contra el actor amenaza. La incertidumbre se representa a menudo usando la probabilidad de ocurrencia o probabilidad.

#### 2.1.32 Estrategia de Protección

Define la estrategia general empleada por una organización para permitir, iniciar, implementar y mantener su seguridad interna. Se estructura en función de las áreas de práctica de seguridad.

#### 2.1.33 Característica

Una cualidad o atributo de una zona de prácticas de seguridad. Cada zona de prácticas de seguridad comprende múltiples características.

#### 2.1.34 Enfoque

La manera en que una organización se ocupa de una característica de una zona de prácticas de seguridad.

#### 2.1.35 Tarea

Una actividad que debe ser completado como parte de una zona de prácticas de seguridad operacional.

#### 2.1.36 Áreas de Práctica de Seguridad

Grupos de prácticas que son estratégicas u operativas. Las áreas estratégicas de práctica de seguridad suelen ser amplios y tienden a afectar todos los riesgos a todos los activos críticos por igual (por ejemplo, la documentación de un conjunto de políticas de seguridad para la organización). Las áreas operacionales de práctica de seguridad se centran en las tareas del día a día y pueden ser dirigidos a mitigar riesgos específicos de los activos específicos (por ejemplo, la comprobación de un sistema específico para cuentas por defecto).

#### 2.1.37 Enfoque Mitigación

Cómo una organización tiene la intención de abordar un riesgo. Una organización tiene las siguientes opciones para cada riesgo: aceptar, mitigar o retrasar.

#### 2.1.38 Aceptar

Una decisión tomada durante el análisis de riesgo a tomar como decisión ninguna medida de control para hacer frente a un riesgo y aceptar las consecuencias si ocurre el riesgo. Los riesgos que se aceptan generalmente tienen un bajo impacto en una organización.

#### 2.1.39 Mitigar

Una decisión tomada durante el análisis de riesgos para hacer frente a un riesgo mediante la implementación de actividades diseñadas para contrarrestar la amenaza subyacente. Los riesgos que se mitigan suelen tener un alto impacto en una organización.

#### 2.1.40 Aplazar

Una situación en la que el riesgo ni ha sido aceptado ni mitigado. El impacto en la organización, debido al riesgo diferido está por encima de un umbral mínimo, pero no tan grande como para ser una prioridad inmediata. Riesgos diferidos se observaron y reevaluados en algún momento futuro.

#### 2.1.41 Área de Mitigación

Una zona de prácticas de seguridad que está designado para ser mejorada con el fin de mitigar uno o más de los riesgos de seguridad de una organización.

#### 2.1.42 Plan de mitigación del riesgo

Un plan que tiene por objeto reducir los riesgos a un activo crítico. Los planes de mitigación de riesgos tienden a incorporar actividades o medidas, destinadas a contrarrestar las amenazas a esos activos.

### 2.2 Estado del Arte

Basados en el Modelo para la Investigación Documental propuesto en [3], se presentan documentos que involucran el análisis y gestión del riesgo en un SGSI, teniendo en cuenta la norma ISO 27001, ISO 27005, y algunas actividades adicionales que fortalecen dicho sistema. Estos documentos se muestran clasificados en tres grupos según su objeto de estudio: gestión del riesgo, implantación de un SGSI, y metodologías de análisis y gestión de riesgos.

#### 2.2.1 Gestión del riesgo

En [4], se argumenta que uno de los problemas más importantes con el estado actual de la gestión de riesgos de la información es la falta de nomenclatura establecida. Términos como "amenaza", "impacto", e incluso "riesgo" pueden llevar a diferentes perspectivas y significados. Debido a esto, el autor realiza una conciliación de términos en una taxonomía y ontología común, para que una vez comprendidos se proceda a revisar la norma ISO/IEC 27005.
Además, en [5], [6], [7], se presentan conceptos y definiciones referentes a la gestión del riesgo de TI[5], así como los principales pasos en un análisis de riesgos de TI. Además exponen las regulaciones y normas que tratan el riesgo junto con las principales metodologías de análisis. De forma similar, en [8] se realiza una conceptualización de actividades concernientes al análisis del riesgo y las estrategias de respuesta para diferentes tipos de riesgos.
Por otra parte, en [9] se presenta una visión general del proceso descrito en la norma ISO/IEC 27005:2008, proponiendo el uso de estándares de seguridad para cumplir con las directrices de dicha norma, lo cual facilita el desarrollo de

[5] Tecnologías de la información

metodologías para la gestión de riesgos a través de la combinación de patrones y actividades que se especifican en ISO/IEC 27005. Para esto, los patrones están asociados a las actividades de la norma. Dicha asociación puede facilitar el proceso de desarrollo de la misma, aportando mayores garantías al uso de las mejores prácticas.

En [10], se tiene como objetivo analizar los riesgos y vulnerabilidades existentes dentro de la red de datos de la Escuela Politécnica Nacional. Para ello, realizan un análisis de las Metodologías para el análisis de riesgos y vulnerabilidades de TI más representativas. Entre ellas se analizaron Cobit, varios estándares NIST, OCTAVE-S, y por ultimo OCTAVE; siendo esta última la herramienta sobre la cual se fundamentó la elaboración del proyecto. Finalmente se formulan conclusiones y recomendaciones referentes a la aplicación de OCTAVE en el cumplimiento de su objetivo, resaltando la perfecta aplicabilidad que tuvo dicha metodología.

Adicionalmente, en [11] se realiza un análisis de riesgos informáticos y la elaboración de un plan de contingencia siguiendo la metodología OCTAVE, que fue seleccionada para su proyecto luego de evaluar las principales metodologías para el análisis y gestión del riesgo. Además, el autor da a conocer recomendaciones para proyectos futuros en los que se pueda adaptar la metodología de análisis y gestión de riesgos OCTAVE.

Por otro lado, en [12] se realiza un plan de seguridad de la información para un caso simulado, planteando una metodología para dicho plan, así como los resultados de las diferentes fases de recolección y análisis de información. El estudio define criterios para identificación, caracterización y tipificación de activos, útiles para el presente TFM. Similarmente, en [13] se estudian diferentes enfoques de estándares desarrollados para gestionar la seguridad de la información. Se analizan diferentes métodos conocidos de análisis y gestión de riesgos, algunos de ellos promovidos por gobiernos y/o industria de países de vanguardia y trayectoria reconocida en la seguridad de la información que han tenido gran aceptación. Adicionalmente se presenta una metodología que busca integrar lo mejor de cada uno de los enfoques estudiados. Finalmente se analiza la aplicación de la metodología a un caso de estudio, analizando las particularidades de éste último.

### 2.2.2 Implantación de un SGSI

En [14], se muestran etapas en las que se define de manera general el proceso de implantación y certificación de un Sistema de Gestión de Seguridad de la Información, indicando el uso de metodologías para el análisis, gestión de riesgos, e identificación de activos de información. De igual modo, en [15] se presenta el desarrollo de un marco conceptual y metodológico para la etapa de estableci-

miento de un SGSI bajo la perspectiva de las prácticas sugeridas por el estándar ISO 27001:2005. El estándar exige como punto de partida para establecer el SGSI que la empresa: "defina el alcance del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología" (ISO, 2005). Para cumplir con lo anterior, el autor usa la Metodología de las Elipses propuesta en [16] como herramienta de identificación de los componentes de cada proceso y las interacciones con otros procesos en la organización y con entidades externas a la empresa.

Por otra parte, en [17] se muestra un estudio completo para el establecimiento de un SGSI en un sistema de información, tomando como caso de estudio el Sistema Administrativo Integrado (SAI) de la Universidad Nacional Experimental Politécnica Antonio José de Sucre (UNEXPO), en el cual expresan los beneficios al implantar un SGSI. Además por medio de las fases de Diagnóstico y factibilidad formulan las necesidades que pueden existir en un ente universitario.

Para determinar el alcance del SGSI e identificar interfaces, interdependencias con áreas y procesos de UNEXPO, se plantea el uso de la Metodología de las Elipses propuesto en [16], Por lo anterior, este estudio es de gran importancia para el presente TFM, ya que se usó la Metodología de las Elipses y funcionó exitosamente en el SGSI de aquella Universidad, además, el caso de estudio se encuentra clasificado en el sector educativo, que es el mismo sector donde se sitúa la Universidad del Cauca.

Adicionalmente, en [18] se muestra un caso real en la Banca Latinoamericana. Se detallan los pasos metodológicos seguidos para identificar el alcance para establecer el estándar ISO 27001:2005 en el proceso de "cuentas corrientes", recomendando utilizar el Método de las elipses para visualizar con mucha precisión los distintos subprocesos que componen el alcance del modelo, e identificar los activos de información existentes en dicho alcance. Por lo anterior aplicamos el método de las elipses para definir el alcance en nuestro *caso de estudio*.

### 2.2.3 Metodologías de análisis y gestión de riesgos.

En [19], el autor muestra qué tipo de estándares y normas se deben considerar para llevar a cabo un análisis de riesgos; además, explica cómo articular y utilizar una metodología en el proceso de gobernabilidad de Tecnologías de la Información. Además, el documento da una pauta de cómo realizar el tratamiento del riesgo teniendo en cuenta los cuatro enfoques tradicionales que la norma ISO 27005 da al respecto: establecer controles, aceptar el riesgo, eliminar el riesgo, y trasladar el riesgo.

En [20], se presenta una metodología para gestionar riesgos tecnológicos cuya base son los estándares ISO 31000 e ISO/IEC 27005. Además incluye recomendaciones y buenas prácticas de otros estándares y guías internacionales para

manejo de riesgos, seguridad y gestión de servicios. La metodología se desarrolla para riesgo tecnológico dado que el aumento en el uso de tecnologías de la información posibilita puntos de quiebre o fisuras en aspectos de seguridad con respecto a su utilización, por ello se presenta una forma de aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva tecnológica.

Por otra parte, en [21] el autor propone como eje central una descripción detallada de trece metodologías que sirven como guía para el análisis de riesgos. El documento presenta tablas comparativas de dichas metodologías, teniendo en cuenta veintiocho criterios principales para evaluar sus componentes y características.

Análogamente, en [11] se realiza un estudio comparativo de las principales metodologías para el análisis de riesgos, así como también se realiza un estudio comparativo de las metodologías para la elaboración de un plan de contingencia, con el fin de seleccionar la más apropiada para llevar a cabo la gestión del riesgo en la empresa eléctrica Quito S.A. Como conclusión los autores probaron que la metodología OCTAVE es la más adecuada para realizar proyectos como el de su caso de estudio. De igual forma, presenta una visión de dicha metodología, describiendo el desarrollo con sus tres fases de trabajo, características, y casos de éxito a nivel internacional, sugiriendo que dicha metodología es un buen complemento para implementar metodologías como ITIL o COBIT.

De forma similar, en [22] se presentan los resultados obtenidos tras realizar una revisión sistemática de metodologías y modelos para el análisis de riesgos, que tengan en cuenta riesgos jerárquicos y asociativos para Pequeñas y Medianas Organizaciones (PYMES). Asimismo, en [7] se realiza una propuesta metodológica para llevar a cabo una auditoría soportada en el análisis de riesgos que los autores consideran susceptible de ser utilizada en PYMES.

Dentro de este contexto, en [23] se plantea como objetivo mejorar la Gestión de la Seguridad de los Sistemas de Información y Comunicaciones de la Administración Pública Federal. Reúne conceptos de la gestión de riesgos y presenta un estudio comparativo de las principales metodologías y herramientas de análisis y gestión de riesgos existentes en el mundo, sirviendo como un instrumento de evaluación que puede ser utilizado en la elección de la metodología a ser aplicada por los organismos de la Administración Pública Federal. Los resultados de este documento son un inventario de herramientas, metodologías y cuadros comparativos que destacan algunas de sus cualidades y beneficios. El estudio de estas normas, metodologías y herramientas demuestra una tendencia a la convergencia y la integración entre ellas.

De forma similar, en [24] se tiene como objetivo general aplicar la norma OCTAVE-S en la empresa Pirámide Digital para realizar una evaluación del manejo de riesgo en seguridad informática. El autor realiza un cuadro comparativo entre OCTAVE-S, ISO 17799 y COBIT 4.1, con la descripción de esa tabla se justifica el porqué de la elección de OCTAVE-S para realizar el análisis de riesgos en la organización.
En [25], se presentan ejemplos de hojas de cálculo con los perfiles de riesgo y la documentación que se obtiene al aplicar las tres fases de OCTAVE. El autor justifica la elección de dicha metodología debido a la gran capacidad de configuración que ésta permite. Finalmente confirma que los resultados obtenidos del análisis fueron eficaces, comprensibles y utilizables.

### 2.2.4 Conclusiones del estado del arte

Los documentos presentados en el estado del arte conforman la base para llevar a cabo la propuesta de este TFM, ya que sirven como guía en la definición de las actividades de gestión de riesgos de acuerdo con la norma ISO/IEC 27005. Además muestran la aplicación de metodologías para el análisis y gestión de riesgos que han sido modificadas e implementadas en el contexto de diferentes organizaciones.
Siguiendo los estudios y recomendaciones presentes en [10], [11], [21], [24], se concluye que la **metodología OCTAVE-S** es la adecuada para aplicar al *caso de estudio*.
Los documentos [15], [17], [18], justifican que la **Metodología de las Elipses** propuesta en [16], es la más apropiada para llevar a cabo la definición del alcance de un SGSI. Por lo tanto, será aplicada para tal fin en el presente TFM.
Se debe tener en cuenta que la etapa de plan según la norma ISO/IEC 27001, permite el establecimiento de un SGSI, la cual da la pauta de la estructura de este y sirve para el desarrollo de la ISO/IEC 27005 que es la aplicada en este TFM.

# 3 Caso De Estudio[6]

Lo primero que se realizó fue la recolección de información referente al proceso Inscripciones y Admisiones. Luego se procedió a crear la documentación del mismo debido a que no existía de manera detallada, obteniendo siete procedimientos, los cuales son los siguientes:

1. Definición del calendario de admisión
2. Justificación del servicio de aplicación de la prueba
3. Inscripciones
4. Alistamiento para la aplicación de la prueba
5. Aplicación de la prueba
6. Evaluación de la prueba
7. Admisiones

Cada procedimiento cuenta con una serie de actividades las cuales se deben llevar a cabo para cumplir sus objetivos. A continuación se dará una descripción de las actividades de cada procedimiento:

## 3.1 Definición del calendario de admisión

Las actividades de este procedimiento son las siguientes:

1. **Estudiar el calendario académico**: Se hace con base en las fechas institucionales y se verifica que no exista ningún cruce de actividades o cese de actividades.
2. **Realizar el cronograma de admisiones propuesto por DARCA**: DARCA define cuales son las fechas del cronograma de admisiones, teniendo en cuenta los tiempos de cada proceso. Los procesos cambian de acuerdo a lo implementado.
3. **Enviar al Vicerrector académico el cronograma propuesto en Admisiones**: Se envía el cronograma vía correo electrónico con una comunicación sencilla. Además, debe quedar definido antes del día en que se realiza la reunión de consejo académico.
4. **Enviar al Consejo Académico la propuesta para la aprobación**: El vicerrector Académico propone el calendario ante el Consejo Académico para su aprobación.
5. **Aprobar el calendario de admisiones**: El consejo académico en sesión aprueba el calendario propuesto.

[6] Proceso Inscripciones y Admisiones, de la División de Admisión Registro y Control Académico (DARCA) de la Universidad del Cauca; siguiendo las directrices de la norma ISO/IEC 27005:2011

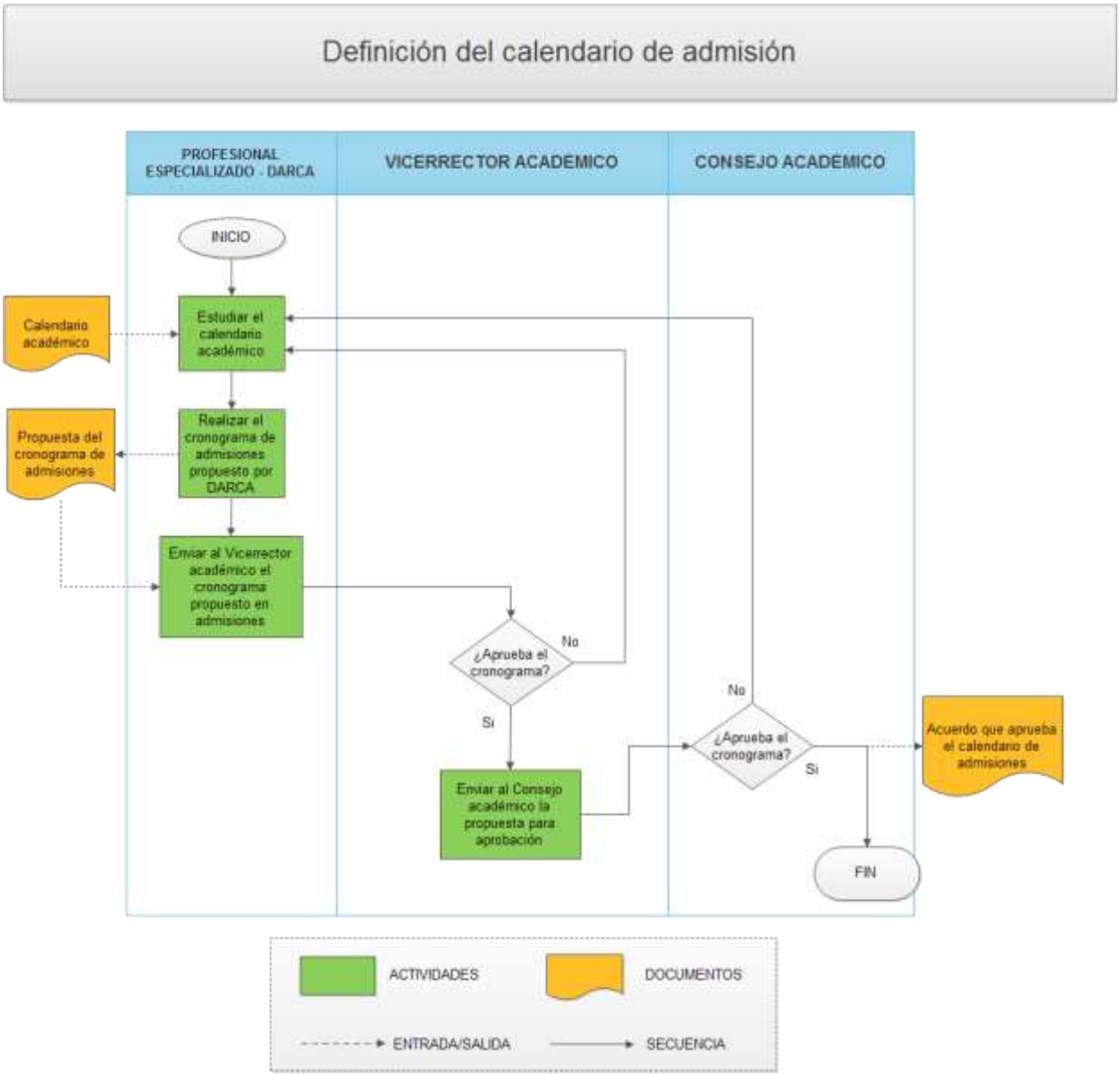


**Ilustración 1. Definición del Calendario de Admisión**

### 3.2 Justificación del servicio de aplicación de la prueba

Las actividades de este procedimiento son las siguientes:

1. **Elaborar el certificado de conveniencia y oportunidad**: La división de admisiones elabora el certificado y lo adjunta en la carpeta del convenio para que la oficina jurídica realice el estudio de la propuesta.
2. **Solicitar certificado de viabilidad técnica al Vicerrector académico**: Se envía físicamente un oficio al vicerrector académico solicitando la viabilidad técnica.
3. **Solicitar certificado de viabilidad financiera**: Se envía físicamente un oficio al Jefe de oficina de planeación solicitando la viabilidad financiera.

4. **Solicitar certificado de conveniencia administrativa**: Se envía físicamente un oficio al Vicerrector Administrativo solicitando el certificado de conveniencia administrativa.
5. **Solicitar el certificado de disponibilidad presupuestal (CDP)**: Se envía físicamente un oficio al Vicerrector Administrativo solicitando el certificado de disponibilidad presupuestal. Después del visto bueno por parte del Vicerrector, se entrega a la oficina financiera.


**Ilustración 2. Justificación del Servicio de Aplicación de la Prueba**

### 3.3 Inscripciones

Las actividades de este procedimiento son las siguientes:

1. **Configurar costos de inscripción**: Ajustar la base de liquidación para la generación de los archivos de inscripción.
2. **Configurar los programas a ofertar**: Consejo académico expide un acuerdo con los programas a ofertar y sus respectivos cupos.
3. **Alistar la plataforma SIMCA**: Desplegar en la web la plataforma de inscripciones.
4. **Abrir inscripciones**: La plataforma queda disponible para las inscripciones.
5. **Cerrar inscripciones**: La plataforma deja de estar disponible para inscripciones.

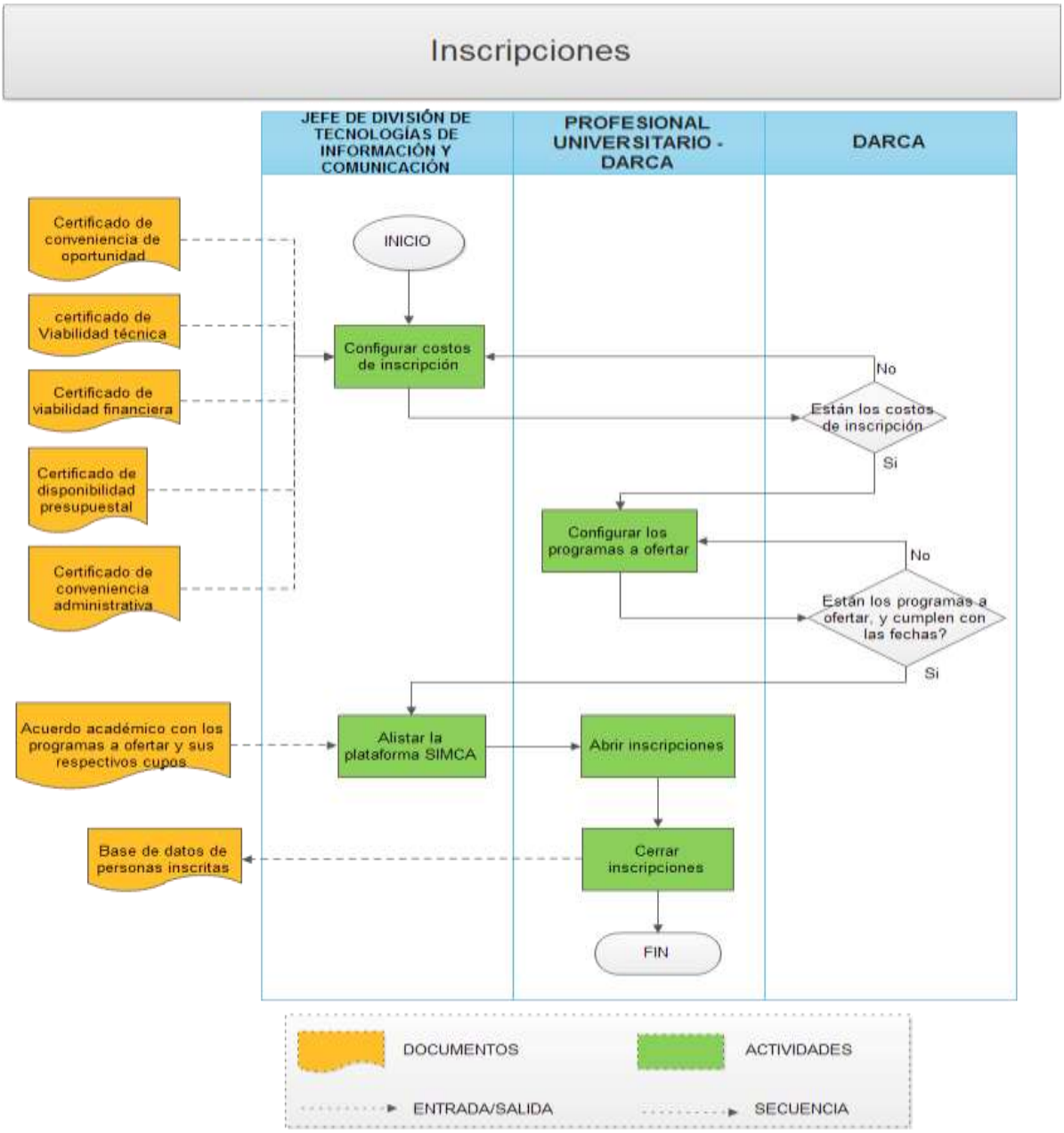


**Ilustración 3. Inscripciones**

### 3.4 Alistamiento para la aplicación de la prueba

Las actividades de este procedimiento son las siguientes:

1. **Consolidar la base de inscripción para la aplicación de prueba**: Se confronta el número de inscripciones frente al número de personas inscritas.
2. **Verificar capacidad instalada y condiciones de infraestructura para la aplicación de la prueba**: Se solicita a cada facultad el número de salones y capacidad en cada uno de ellos. Luego se realiza una visita para verificar el estado de cada salón.

3. **Generar credenciales de citación**: Se genera una sola citación por cada tercero.
4. **Publicar las citaciones**: A través de la plataforma se publica el sitio y la jornada para la presentación de la prueba.
5. **Rotular los puestos para la presentación de la prueba**: Un día antes de la presentación de la prueba, se rotula cada uno de los puestos con la información correspondiente al aspirante y jornada.
6. **Gestionar apoyos para la seguridad de la prueba**: Un mes antes de la presentación de la prueba, se envían solicitudes de apoyo a: Policía metropolitana, Policía de menores, CTI, Vigilancia privada, Cruz roja, Brigada Unicauca.
7. **Solicitar la contratación de dactiloscopistas**: Se solicita a vicerrectoria administrativa la contratación de personal dactiloscopista a través de un CDP.
8. **Asignar y citar el personal de apoyo para la custodia de la prueba**: Se citan los docentes encargados de la custodia de la prueba de acuerdo a la información suministrada por parte de recursos humanos.

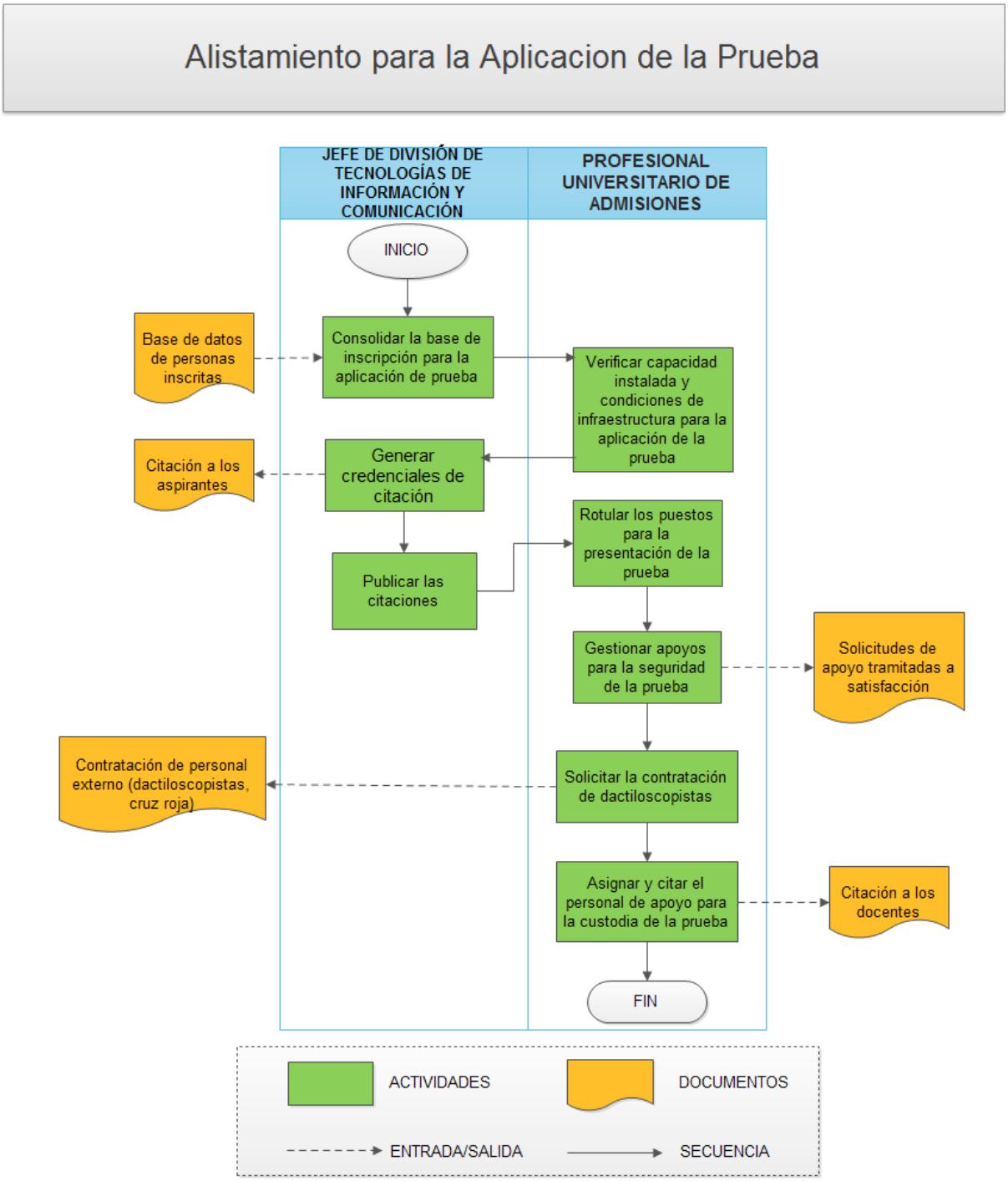


**Ilustración 4. Alistamiento para la Aplicación de la Prueba**

### 3.5 Aplicación de la prueba

Las actividades de este procedimiento son las siguientes:

1. **Verificar la presencia y ubicación del personal de apoyo**: Se solicita la confirmación de la presencia del personal vía radioteléfono.

2. **Permitir ingreso**: Se da la orden para el ingreso de los aspirantes y se verifica su documento de identidad y citación.
3. **Entregar y distribuir el material a los coordinadores de aula**: El personal de admisiones hace entrega a los coordinadores del material para la aplicación de la prueba (FORMULARIOS Y TARJETAS DE RESPUESTAS).
4. **Entregar el material (formularios y tarjetas de respuestas) a los aspirantes**: Cada jefe de aula entrega de manera individual el formulario y tarjeta de respuestas.
5. **Iniciar la prueba**: Se garantiza el tiempo estimado para el desarrollo de la prueba.
6. **Llevar a cabo a el registro dactiloscópico**: Antes de terminar el tiempo destinado para la prueba, cada aspirante debe haber impreso su huella en el formulario.
7. **Diligenciar formato A1**: Cada jefe de aula diligencia un formato que contiene la información relacionada con el número de tarjetas recibidas y entregadas.
8. **Finalizar prueba**: Se da por terminada la jornada manifestándose a los aspirantes.
9. **Realizar anulación de formularios y hojas de respuestas no utilizadas**: Cada jefe de aula procede con la anulación escribiendo "anulado" en la hoja de respuesta y diligencia el formato A1.
10. **Entregar formatos A1 diligenciados y tarjetas de respuestas anuladas**: Cada jefe de aula entrega los formatos A1 y las tarjetas de respuestas anuladas al coordinador de aulas.
11. **Empacar y colocar sellos de seguridad**: material, los coordinadores se dirigen a un recinto donde el material es empacado y sellado.
12. **Cerrar actividades de la jornada**: Se realiza una reunión con los representantes de los principales actores del proceso para evaluar el desarrollo de la prueba.

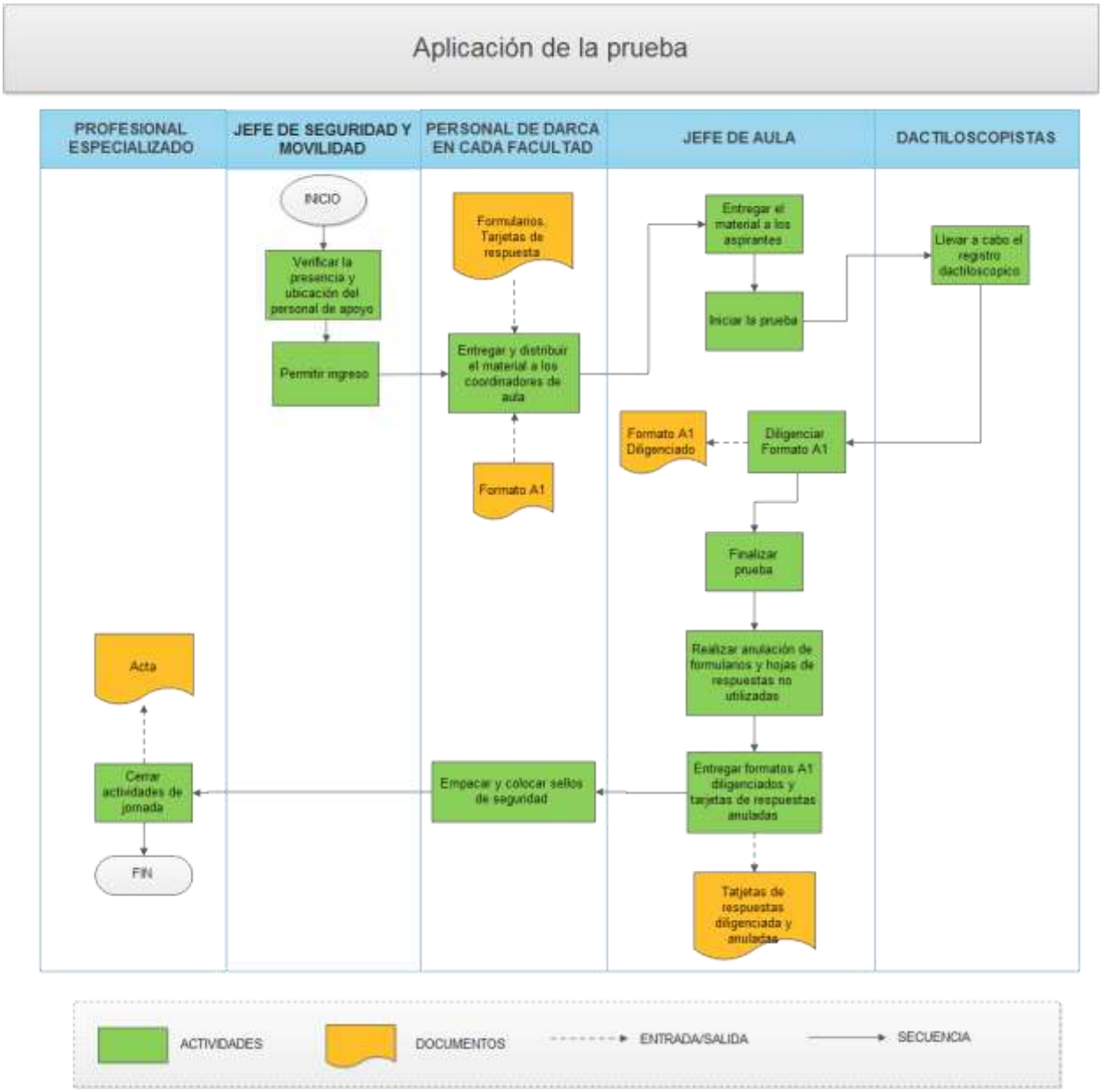


**Ilustración 5. Aplicación de la Prueba**

### 3.6 Evaluación de la prueba

Las actividades de este procedimiento son las siguientes:

1. Abrir los paquetes que contienen las tarjetas de respuesta debidamente diligenciadas: Al menos dos (2) representantes de la Universidad del Cauca verifican la apertura de los paquetes que contienen las hojas de respuesta para su posterior calificación.
2. Generar claves de respuesta: Los cuestionarios son resueltos posteriormente a la aplicación de la prueba, insumo necesario para la generación de claves o respuestas.

3. Parametrizar el sistema: Con base en las claves de respuestas se parametriza el sistema que realizará la calificación.
4. Leer las hojas de respuesta: Se ingresan las hojas de respuesta en la máquina lectora para su calificación.
5. Ordenar los puntajes en orden descendente por programa: De acuerdo a la calificación, los aspirantes son ordenados en estricto orden descendente.
6. Cargar los resultados en SIMCA: El resultado del ordenamiento es cargado en SIMCA para la posterior selección.
7. Determinar el mínimo de admisión: Los datos correspondientes al puntaje mínimo y máximo son enviados al consejo académico para definir el mínimo de admisión.
8. Seleccionar aspirantes: Con base en el ordenamiento, el puntaje mínimo de admisión, y el número de cupos por programa, son seleccionados los aspirantes admitidos.
9. Alistar la plataforma de publicación de resultados: Se realiza el despliegue de los servidores para la publicación de las listas.
10. Revisar los datos a publicar: Se realiza una revisión por programa de acuerdo a los cupos, empates y puntaje obtenido.
11. Publicar los resultados: La lista de admitidos se despliega para poder ser consultada por los usuarios.

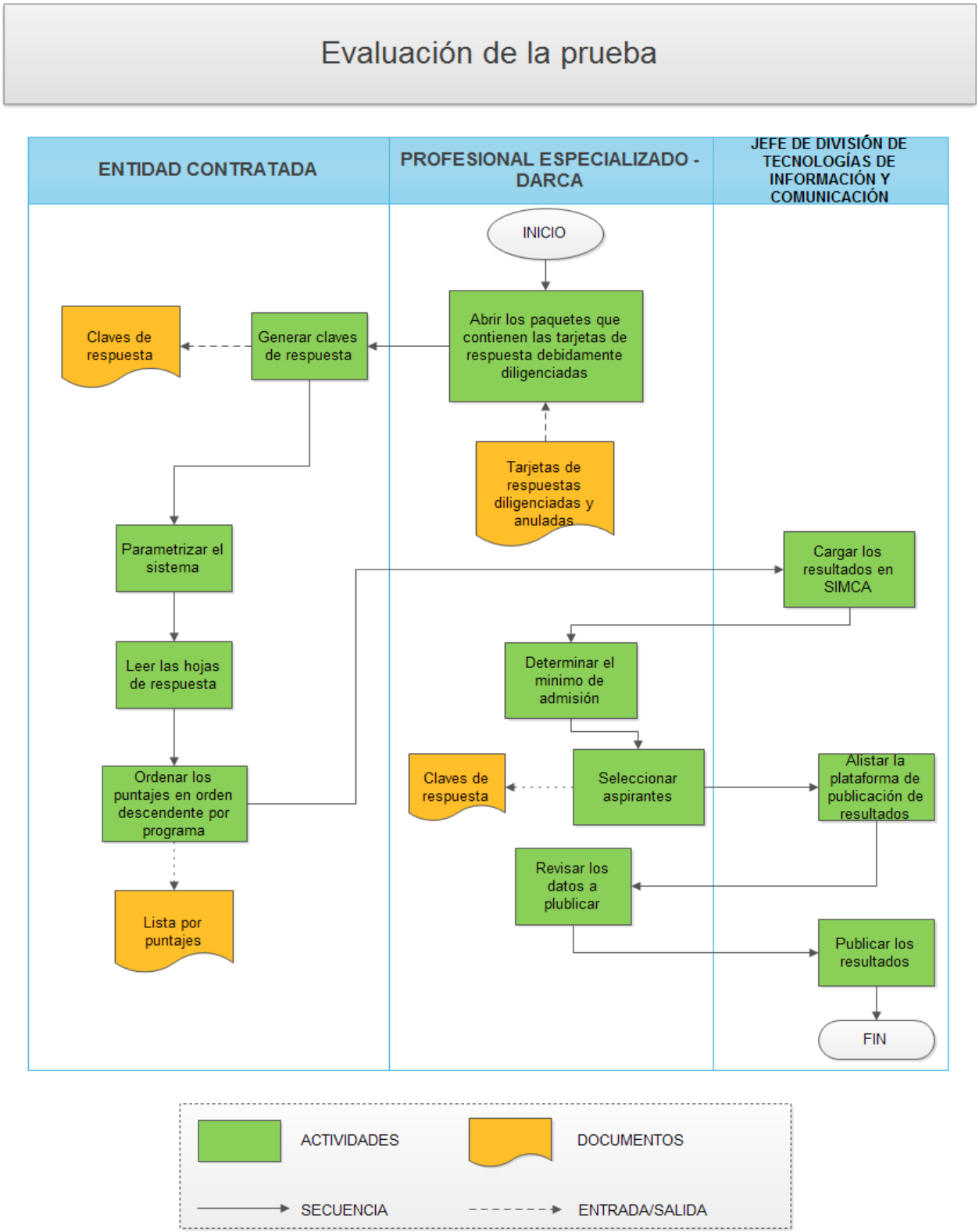


**Ilustración 6. Evaluación de la Prueba**

Siler Amador Donado
D.N.I 72.168.640

### 3.7 Admisiones

Las actividades de este procedimiento son las siguientes:

1. **Alistar la plataforma de liquidación**: La plataforma se ajusta con base a los datos de liquidación de la vigencia.
2. **Recibir documentación**: Se realiza la recepción documental de acuerdo a la lista de chequeo.
3. **Liquidar los derechos de matrícula**: De acuerdo a la documentación aportada se realiza la matrícula financiera (recibo de pago).
4. **Cerrar primer llamado de admisión**: Luego de vencidos los términos de pago de matrícula financiera se realiza el alistamiento para el segundo llamado.
5. **Abrir segundo llamado de admisión**: De acuerdo a los cupos liberados se configura el segundo llamado de admisión.
6. **Cerrar proceso de admisión**: Realizar el cierre del proceso para la posterior matrícula académica.
7. **Realizar Matrícula académica**: Se matricula a los estudiantes que cumplen con el requisito de matrícula financiera en los términos establecidos.

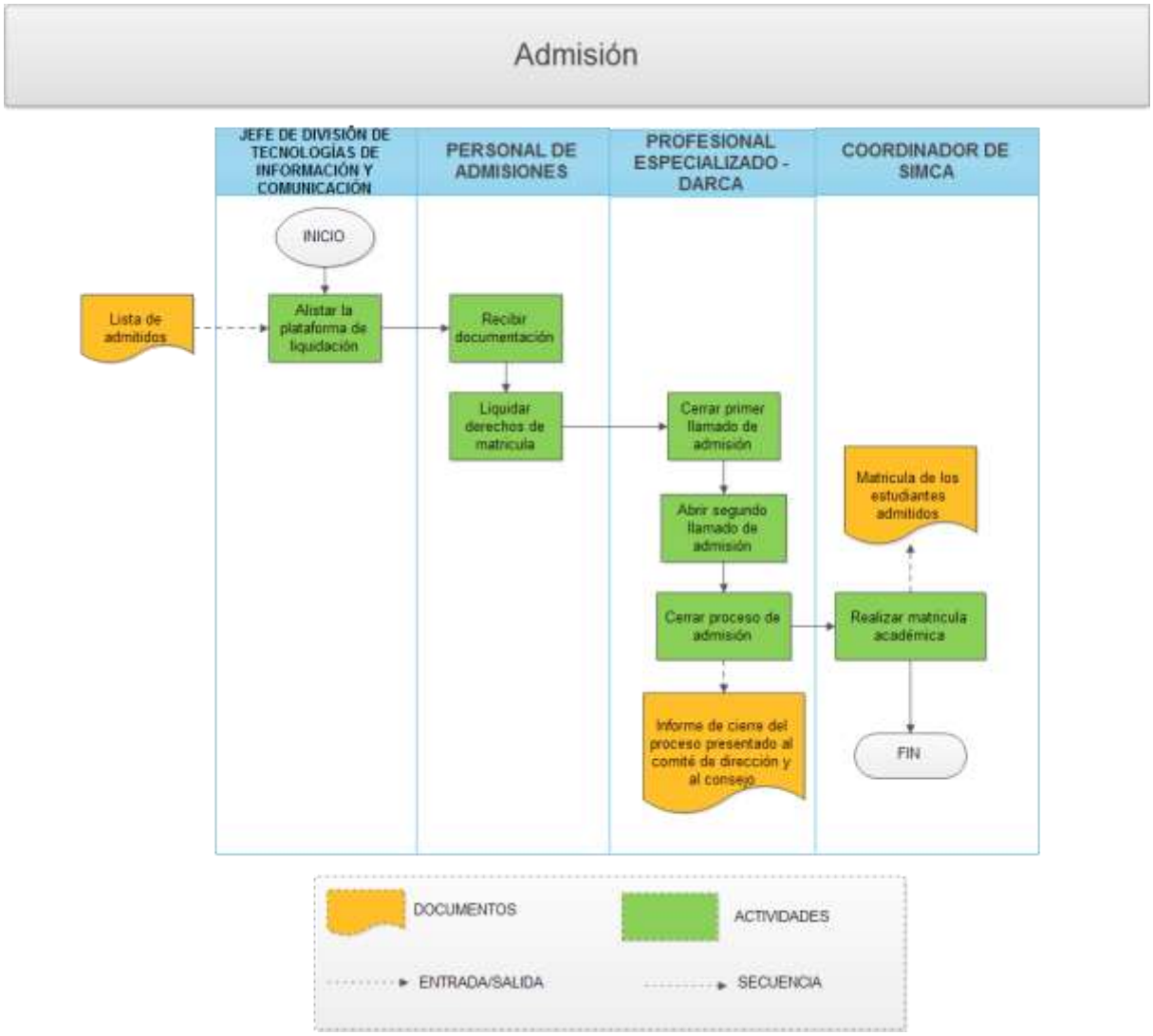


**Ilustración 7. Admisión**

Luego de haber documentado todo el proceso del *caso de estudio*, se especificó en diagramas el orden de las actividades para un rápido entendimiento. Los diagramas están en los anexos.

A continuación y con ayuda de la metodología de las Elipses, se realizó el alcance del proceso Inscripciones y Admisiones. En este se muestra además de los procedimientos del proceso, todas las entidades o cargos involucrados para cada procedimiento. En los anexos se encuentra el diagrama del alcance.

Siler Amador Donado
D.N.I 72.168.640

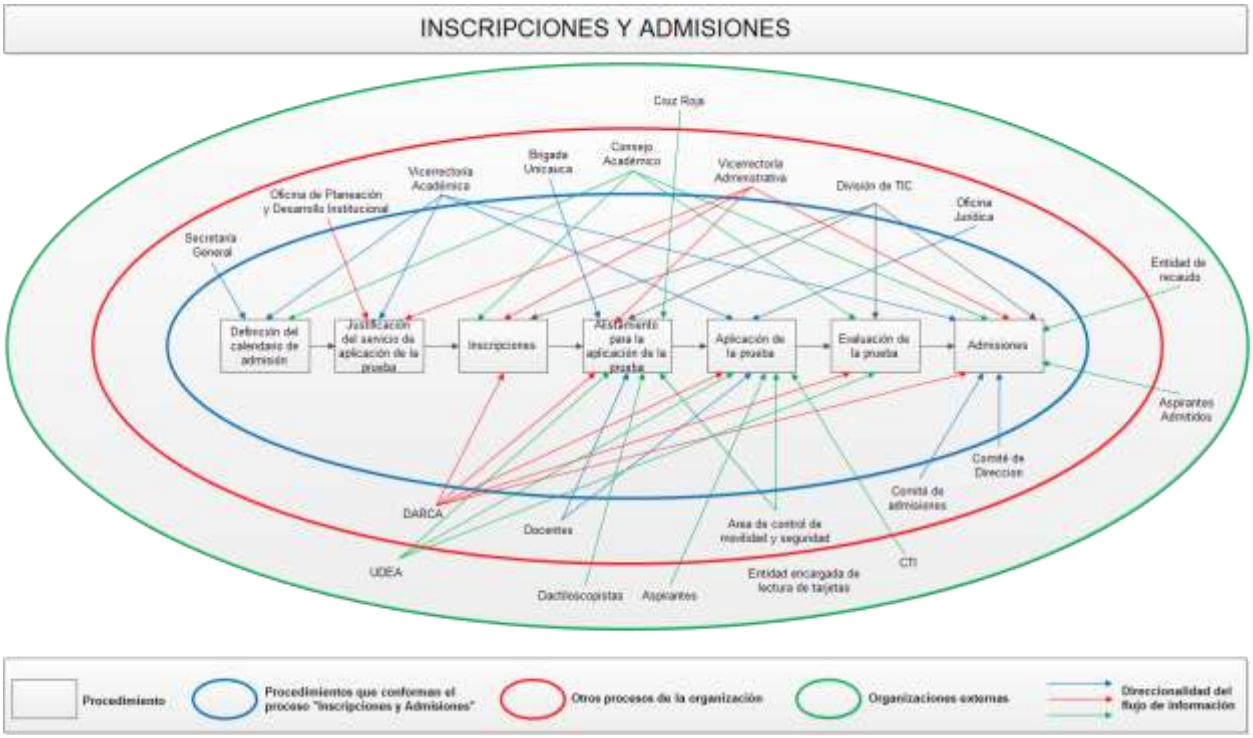


**Ilustración 8. Metodología de las Elipses en Inscripciones y Admisiones**

Siler Amador Donado
D.N.I 72.168.640

# 4 Metodología de análisis y gestión del riesgo OCTAVE-S

Para una organización que busque comprender sus necesidades de seguridad de la información, **OCTAVE** (**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation) es una técnica de evaluación y planificación estratégica basada en el riesgo para la seguridad, fue desarrollada en el año 2001 por la universidad Carnegie Mellon para el Departamento de defensa de los Estados Unidos. Existen dos versiones: **OCTAVE-S**, es una metodología simplificada para las organizaciones más pequeñas que tienen estructuras jerárquicas planas, y **OCTAVE Allegro**, es una versión más completa para las organizaciones grandes o aquellos con estructuras de varios niveles. OCTAVE es auto dirigido, lo que significa que las personas de una organización asumen la responsabilidad de establecer la estrategia de seguridad de la organización. La técnica aprovecha los conocimientos de las prácticas y los procesos relacionados con la seguridad de su organización para capturar el estado actual de la seguridad dentro de la organización. Los riesgos para los activos más críticos se utilizan para priorizar áreas de mejora y establecer la estrategia de seguridad de la organización. A diferencia de las evaluaciones centradas en la tecnologías típicas, las cuales están dirigidas a riesgo tecnológico y se centraron en cuestiones tácticas, OCTAVE está dirigido a riesgo de la organización y se centró en temas estratégicos, relacionados con la práctica. Es una evaluación flexible que se puede adaptar para la mayoría de las organizaciones. El enfoque OCTAVE es impulsada por dos de los aspectos: el riesgo operativo y las prácticas de seguridad. La tecnología sólo se examina en relación con las prácticas de seguridad, lo que permite a una organización afinar la vista de sus prácticas de seguridad actuales. Al utilizar el enfoque OCTAVE, una organización toma decisiones de protección de la información basada en los riesgos para la **confidencialidad**, **integridad** y **disponibilidad** de los activos relacionados con la información crítica. Todos los aspectos de riesgo (*activos*, *amenazas*, *vulnerabilidades* y el *impacto* sobre la organización) se tienen en cuenta en la toma de decisiones, lo que le permite a una organización que coincida con una estrategia de protección basada en la práctica de sus riesgos de seguridad.

Las siguientes son las fases que conforman OCTAVE-S:

### 4.1 Fase 1. Construir perfiles de amenazas basadas en los activos del caso de estudio[7]

En esta fase se realizó una evaluación de los aspectos organizacionales en DARCA con respecto al proceso Inscripciones y Admisiones. Durante esta fase, se definieron los criterios de evaluación de impacto que se utilizarán más adelante para evaluar los riesgos. También se identificaron los activos organizacionales importantes y se evaluaron las prácticas actuales de la seguridad de la organización. A continuación, se seleccionaron *quince activos críticos* para analizarse en profundidad basándose en la importancia relativa a la organización. Finalmente, se definieron los requisitos de seguridad y un perfil de amenaza para cada activo crítico.

1. **Identificar Información del proceso de Inscripciones y Admisiones de DARCA**

En esta parte se centro en el desarrollo de criterios para evaluar el impacto de los riesgos para la organización, la identificación de los activos de la organización, así como la evaluación de las prácticas de seguridad de la organización.

2. **Crear perfiles de amenazas del proceso Inscripciones y Admisiones**

En esta parte se centró en la selección de los activos críticos de los previamente identificados, la identificación de requisitos de seguridad para los activos y la identificación de las amenazas a los activos críticos.

### 4.2 Fase 2. Identificar las vulnerabilidades de la infraestructura con respecto al *caso de estudio*

Durante esta fase, se llevó a cabo una revisión de alto nivel de la infraestructura informática de DARCA, centrándonos en la medida en que la seguridad es considerada por los asistentes de la infraestructura. Primero se analizó cómo las personas usan la infraestructura informática para acceder a los activos críticos,

[7] Proceso Inscripciones y Admisiones de DARCA (División de Admisión Registro y Control Académico) de la Universidad del Cauca; siguiendo las directrices de la norma ISO/IEC 27005:2011

dando clases principales de componentes, así como quién es responsable de la configuración y el mantenimiento de esos componentes.
Posteriormente, se examinó el grado en que cada uno de los responsables incluye la seguridad en sus prácticas y procesos de tecnología de la información con respecto al proceso de *Inscripciones y Admisiones*.

1. **Examinar la Infraestructura Informática en relación con los activos críticos.**

En esta fase se examinaron las vías de acceso en la infraestructura para los activos críticos y luego se analizó la tecnología relacionada con los procesos asociados con la infraestructura.

### 4.3 Fase 3. Desarrollo de Estrategia y Planes de Seguridad

Durante esta fase se identificaron los riesgos sobre los activos críticos de la organización y se decidió qué hacer con ellos. Sobre la base de un análisis de la información recopilada, se creó una estrategia de protección para los planes de organización y de mitigación para hacer frente a los riesgos de los activos críticos.

1. **Identificar y analizar los riesgos.**

En esta etapa se realizó la evaluación del impacto y probabilidad de las amenazas sobre los activos críticos y el establecimiento de criterios de evaluación de la probabilidad.

2. **Desarrollar estrategia de protección y planes de mitigación**

En esta etapa se estableció la definición de una estrategia de protección y planes de mitigación, así como los próximos pasos necesarios para poner en práctica los resultados de la evaluación OCTAVE-S.
Los resultados se describen paso a paso en el capítulo 5.

# 5 Aplicación de las fases de OCTAVE-S al caso de estudio contrastándola con las directrices de la norma ISO/IEC 27005

Las fases de OCTAVE-S fueron contrastadas con la norma ISO/IEC 27005 a medida que se realizaba la gestión del riesgo al *caso de estudio*. Los resultados de cada paso son los siguientes:

## 5.1 Criterios de Evaluación de Impacto (Paso 1)

En este paso se definieron un conjunto de medidas cualitativas contra el cual se evalúo el efecto de cada riesgo en la misión y los objetivos del proceso Inscripciones y Admisiones de DARCA. Se definieron los rangos alto, medio y bajo impacto para el proceso. Se consideraron las siguientes áreas de impacto:

1. **Reputación - Confianza de los Usuarios**: se manejan dos variables, las cuales son reputación y pérdida de usuario(s).
2. **Financiero**: Se manejan tres variables, las cuales son costos operativos, pérdida de ingresos y perdida financiera.
3. **Productividad**: Se maneja una sola variable, la cual es horas de personal.
4. **Seguridad - Salud**: Se manejan tres variables, las cuales son vida, salud y seguridad.

En la siguiente tabla se muestran los criterios de evaluación del impacto (Paso 1) para aplicar sobre el *caso de estudio*:

| **Tipo de impacto** | **Bajo Impacto** | **Medio Impacto** | **Alto Impacto** |
|---|---|---|---|
| Reputación | La reputación se ve afectada mínimamente, se requiere poco o ningún esfuerzo o gasto para recuperarse. | La reputación se daña, y se requiere un poco de esfuerzo y gastos para recuperarse. | La reputación está irrevocablemente destruida o dañada. |
| Perdida | Menos de 5% de reducción en los | 5 a10% de reducción en los usuarios | Más de 10% de reducción en los |

| | | | |
|---|---|---|---|
| Usuario | usuarios debido a la pérdida de confianza. | debido a la pérdida de confianza. | usuarios debido a la pérdida de confianza. |
| Costos Operativos | Aumento de menos de 10% de los costes operativos anuales | Los costos de operación anuales aumentan en 11 a 50%. | Los costos de operación anuales aumentan en más de un 50 %. |
| Pérdida de ingresos | Menos de 10% de pérdida de ingresos anuales | 11 a 50% de pérdida anual de ingresos | Mayor que 51% de pérdida anual de ingresos |
| Pérdida Financiera | Costo financiero de menos de 50 millones de pesos anuales | Costo financiero de primer tiempo de 51a 250 millones de peso anuales | Mayor costo financiero de 250 millones de pesos anuales |
| Horas de Personal | Las horas de trabajo del personal se incrementaron en menos de 10% de 5 a 10 día (s). | Las horas de trabajo del personal se incrementaron entre 11% y 20% de 5 a 10 día (s). | Las horas de trabajo del personal se incrementaron en más de un 21% de 5 a 10 día (s). |
| Vida | No hay pérdida o amenaza significativa a las vidas de los clientes o el personal de los miembros | Vidas de los clientes o de los miembros del personal están amenazadas, pero se recuperarán después de recibir tratamiento médico. | La pérdida de vidas de los clientes o el personal de los miembros |
| Seguridad | Seguridad Cuestio- | Seguridad Afectada | Seguridad Violada |

| | | | |
|---|---|---|---|
| | nada | | |

**Tabla 1. Criterios de Evaluación de Impacto**

### 5.2 Identificación de Activos (Paso 2)

Los activos del *caso de estudio* se clasificaron según las categorías propuestas en ISO/IEC 27002. De esta forma la selección de activos se dividió de la siguiente manera: Activos de Sistemas (activos físicos), Activos de Información, Activos de Aplicaciones (activos de software), Activos de Servicios, Personas Involucradas en el proceso Inscripciones y Admisiones y activos intangibles.

Los activos encontrados son los siguientes:

| **PREGUNTAS** | **RESPUESTAS** |
|---|---|
| ¿Qué sistemas la gente de DARCA necesitan para realizar su trabajo? | Salones, pupitres, radioteléfonos, el sistemas que realiza la calificación de las tarjetas de respuesta (maquina lectora), los servidores que contienen la plataforma para la publicación de las listas. |
| ¿Qué información la gente en DARCA necesitan para realizar su trabajo? | Acuerdo que aprueba el calendario académico, propuesta del cronograma de admisiones, acuerdo que aprueba el cronograma de admisiones propuesto por DARCA, propuesta técnico-económica para el desarrollo de la prueba, solicitud certificado de viabilidad técnica, solicitud de certificado de viabilidad financiera, solicitud certificado de conveniencia administrativa, solicitud certificado de disponibilidad presupuestal (CDP), certificado de viabilidad técnica, certificado de conveniencia |

| | |
|---|---|
| | de oportunidad, certificado de viabilidad financiera, certificado de conveniencia administrativa, certificado de disponibilidad presupuestal (CDP), archivos de inscripción, acuerdo con los programas a ofertar y sus respectivos cupos, resolución que fija los programas y los cupos a ofertar, rótulos con información del aspirante y jornada, credenciales de citación, solicitud de contratación de dactiloscopistas a través de un CDP, citación a los aspirantes, citación a los docentes, contratación de personal externo (dactiloscopistas, cruz roja), solicitudes de apoyo tramitadas a satisfacción, formularios, tarjetas de respuestas, formato a1, tarjetas de respuesta no usadas (anuladas), formatos a1 diligenciados, todo el material empacado y sellado en bolsas de seguridad, acta de cierre de actividades, tarjetas de respuesta diligenciadas y anuladas en paquetes de seguridad, claves de respuesta (respuestas correctas), documento que almacena los puntajes de los aspirantes en orden descendentes, copia del documento que almacena los puntajes de los aspirantes en orden descendentes(se envía a DARCA), archivo cifrado del documento que almacena los puntajes de los aspirantes en orden descendentes cargado en SIMCA[8], datos a publicar (lista de admitidos), documentación de los admitidos, |

[8] Sistema Integrado de Matrícula y Control Académico

| | |
|---|---|
| | datos de liquidación, matrícula financiera(digital), segunda lista de admitidos, matrículas académicas de los estudiantes admitidos, informe de cierre del proceso presentado al comité de dirección y al concejo, y convenio de cooperación interadministrativo suscrito entre la universidad de Antioquia y la universidad del cauca. |
| ¿Qué aplicaciones la gente de DARCA necesitan para realizar su trabajo? | Correo electrónico institucional, sistema integrado de recaudo (SQUID), base de datos de personas inscritas, SIMCA, plataforma de inscripciones, sitio web UNICAUCA, plataforma de inscripciones (repetido), y la plataforma de publicación de resultados. |
| ¿Qué servicios la gente de DARCA necesitan para realizar su trabajo? | Energía eléctrica, aire acondicionado, servicio de internet, red interna, iluminación planta eléctrica. |
| ¿Qué personas tienen una habilidad especial o conocimiento que es vital para su organización y sería difícil de reemplazar? ¿Qué habilidades tienen estas personas? | Ingeniero de soporte (desarrollo), profesional especializado (conocer el proceso y reglamentación institucional), profesional universitario (conocer el proceso y reglamentación institucional), CTI (prevenir fraude), dactiloscopistas (llevar el control de huellas digitales de los aspirantes), cruz roja (auxiliar al aspirante en caso de urgencia de salud). |
| ¿Qué activos intangibles la gente de DARCA necesita para realizar su trabajo? | Reputación e imagen |

**Tabla 2. Identificación de Activos**

### 5.3 Procedimientos de Seguridad (Pasos 3 y 4)

En esta parte se evaluó el grado en que las prácticas de seguridad se reflejan para gestionar la seguridad del *proceso Inscripciones y Admisiones*. Se evaluó con las opciones "Mucho", "Algo, "Nada", y con sus valores respectivos 1, 2, y 3.Con esto se ha podido ver acciones que ayudan a iniciar , implementar y mantener la seguridad dentro del proceso así como las debilidades en la política o en la práctica organizacional que pueden resultar en acciones no autorizadas. También se pudo determinar qué áreas están en riesgo, para más adelante asignarles un color dependiendo del riesgo (Rojo=Alto, Amarillo=Medio, Verde=Bajo). Para realizar la evaluación se tomaron dos tipos de prácticas de seguridad:

1. **Prácticas estratégicas**

Prácticas de seguridad que se centran en cuestiones de organización a nivel de políticas. Estos incluyen problemas relacionados con el proceso, así como cuestiones que requieren los planes y la participación de toda la organización.

2. **Prácticas operacionales**

Prácticas de seguridad que se centran en cuestiones relacionadas con la tecnología. Estos incluyen problemas relacionados con la forma en la gente usa, interactuar con, y proteger la tecnología sobre una base del día a día.

Cada tipo de práctica se divide en áreas, con el fin de evaluar específicamente el proceso de Inscripciones y Admisiones. Las áreas son las siguientes:

3. **Áreas de Prácticas estratégicas:**

   - Conciencia de Seguridad y Formación
   - Estrategia de Seguridad
   - Gestión de la Seguridad
   - Políticas y Reglamentos de Seguridad
   - Gestión de Seguridad Colaborativa
   - Planes de Contingencia/Recuperación de Desastres

4. **Áreas de Prácticas operacionales:**

Siler Amador Donado
D.N.I 72.168.640

- Control de Acceso Físico
- Monitoreo y Auditoría de Seguridad Física
- Gestión de Sistema y Red
- Monitoreo y Auditoría de Seguridad Informática
- Autenticación y Autorización
- Gestión de Vulnerabilidades
- Cifrado
- Diseño y Arquitectura de Seguridad
- Gestión de Incidentes

Los resultados son los siguientes:

**Área 1. Conciencia de Seguridad y Formación:**

| **Enunciado** | **¿Hasta qué punto esta afirmación es reflejada en la organización?** | **Puntaje** |
|---|---|---|
| Los miembros del personal comprenden sus roles y responsabilidades de seguridad. Esto está documentado y verificado | Algo | 2 |
| Hay suficiente experiencia interna para todos los servicios soportados, mecanismos y tecnologías (por ejemplo, logging, la vigilancia o el cifrado), incluyendo su operación segura. Esto está documentado y verificado. | Algo | 2 |
| La conciencia de seguridad, capacitación y recordatorios periódicos se proporcionan para todo el personal. Comprensión personal está documentada y la conformidad es verificada periódicamente. | Algo | 2 |

| | | |
|---|---|---|
| Los miembros del personal siguen las buenas prácticas de seguridad, como: asegurar la información por la cual ellos son responsables, no divulgar información confidencial a otros (resistencia a la ingeniería social), tener la capacidad adecuada para utilizar hardware y software de tecnología de la información, el uso de buenas prácticas de contraseña, entender y seguir las políticas y normas de seguridad, reconocer y reportar incidentes | Algo | 2 |

**Tabla 3. Conciencia de Seguridad y Formación (Área 1)**

**Área 2. Estrategia de Seguridad:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Las estrategias de negocio de la organización incorporan rutinariamente las consideraciones de seguridad. | Mucho | 1 |
| Estrategias y políticas de seguridad tienen en cuenta las estrategias y objetivos de negocio de la organización. | Mucho | **1** |
| Las estrategias de seguridad, las metas y objetivos se documentan y se revisan de forma rutinaria, actualizado, y se comunicarán a la organización. | Nada | **3** |

**Tabla 4. Estrategia de Seguridad (Área 2)**

Siler Amador Donado
D.N.I 72.168.640

**Área 3. Gestión de la Seguridad:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Administración asigna fondos y recursos suficientes para las actividades de seguridad de la información. | Algo | 2 |
| Funciones y responsabilidades de seguridad se definen para todo el personal de la organización. | Mucho | 1 |
| Todo el personal en todos los niveles de responsabilidad pone en práctica sus funciones y la responsabilidad de la seguridad de información asignados. | Algo | 2 |
| Hay procedimientos documentados para la autorización y supervisión de todo el personal (incluido el personal de organizaciones de terceros) que trabajan con información sensible o que trabajan en lugares donde reside la información | Mucho | 1 |
| Las practicas de Contratación y terminación de la organización para el personal toma en cuestión la seguridad de la información en cuenta. | Nada | 3 |
| La organización gestiona los riesgos de seguridad de información, incluyendo: la | Mucho | 1 |

| | | |
|---|---|---|
| evaluación de riesgos para la seguridad de la información, tomar medidas para mitigar los riesgos de seguridad de la información. | | |
| Administración recibe y actúa sobre los informes de rutina que resumen la información relacionada con la seguridad (por ejemplo, auditorías, registros, evaluaciones de riesgo y vulnerabilidad). | Mucho | 1 |

**Tabla 5. Gestión de la Seguridad (Área 3)**

**Área 4. Políticas y Reglamentos de Seguridad:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| La organización cuenta con un amplio conjunto de políticas documentadas, actuales que se revisan y actualizan periódicamente. | Nada | 3 |
| Hay un proceso documentado para la gestión de políticas de seguridad, incluyendo: creación, administración (incluyendo revisiones y actualizaciones periódicas), comunicación. | Algo | 2 |
| La organización cuenta con un proceso documentado para evaluar y garantizar el cumplimiento de las políticas de información de seguridad, las leyes y reglamentos | Nada | 3 |

| | | |
|---|---|---|
| aplicables, y los requisitos de seguro. | | |
| La organización hace cumplir de manera uniforme sus políticas de seguridad. | Nada | 3 |

**Tabla 6. Políticas y Reglamentos de Seguridad (Área 4)**

**Área 5. Gestión de Seguridad Colaborativa:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| La organización cuenta con políticas y procedimientos para proteger la información cuando se trabaja con organizaciones externas (por ejemplo, terceros, colaboradores, subcontratistas o socios), incluyendo: proteger información perteneciente a otras organizaciones, la comprensión de las políticas de seguridad y procedimientos de las organizaciones externas, terminar el acceso a la información por parte de personal externo terminado. | Mucho | 1 |
| La organización documenta los requisitos de protección de la información y las comunica explícitamente a todas las terceras partes apropiadas. | Algo | 2 |
| La organización cuenta con mecanismos formales para verificar que todas las organizaciones de terceros, servicios de seguridad externalizados, mecanismos y tecnologías | Algo | 2 |

| | | |
|---|---|---|
| cumplen sus necesidades y requerimientos. | | |
| La organización cuenta con políticas y procedimientos para colaborar con todas las organizaciones de terceros que: proporcio-nan concienciación sobre la seguridad y los servicios de formación, desarrollan políticas de seguridad para la organización, desarro-llan planes de contingencia para la organización | Nada | 3 |

**Tabla 7. Gestión de Seguridad Colaborativa (Área 5)**

**Área 6. Planes de Contingencia/Recuperación de Desastres:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Se ha realizado un análisis de las operacio-nes, las aplicaciones y la criticidad de los datos. | Algo | 2 |
| La organización ha documentado, revisado y probado: plan (es) de contingencia para responder a las emergencias, plan (es) de recuperación de desastres, los planes de operaciones de emergencia o de continui-dad del negocio. | Nada | 3 |
| Los planes de contingencia, recuperación de desastres y continuidad del negocio consideran requisitos y controles de acceso | Nada | 3 |

| | | |
|---|---|---|
| físicos y electrónicos. | | |
| Todo el personal: conoce de los planes de contingencia, recuperación de desastres y continuidad del negocio, entienden y son capaces de llevar a cabo sus responsabilidades. | Nada | 3 |
| Se identifican los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información. | Nada | 3 |

**Tabla 8. Planes de Contingencia/Recuperación de Desastres (Área 6)**

**Área 7. Control de Acceso Físico:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Los planes y procedimientos para salvaguardar las instalaciones, los edificios y las zonas restringidas de seguridad de las instalaciones están documentados y probados. | Algo | 2 |
| Existen políticas y procedimientos de gestión de | Algo | 2 |

| | | |
|---|---|---|
| visitantes documentados. | | |
| Existen políticas y procedimientos de control de acceso físico a las áreas de trabajo y de hardware (computadoras, dispositivos de comunicación, etc.) y el soporte de software documentados. | Algo | 2 |
| Las estaciones de trabajo y otros componentes que permiten el acceso a la información confidencial estén protegidos físicamente para evitar el acceso no autorizado. | Algo | 2 |
| Los requisitos de la organización para el control de acceso físico se comunicarán formalmente a todos los contratistas y proveedores de servicios que controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software. | Mucho | 1 |
| La organización verifica | Algo | 2 |

| | | |
|---|---|---|
| formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el control de acceso físico. | | |

**Tabla 9. Control de Acceso Físico (Área 7)**

**Área 8. Monitoreo y Auditoría de Seguridad Física:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Los registros de mantenimiento son guardados para documentar la reparación y las modificaciones de los componentes físicos de una facilidad. | Mucho | 1 |
| Las acciones de un individuo o grupo, en lo que concierne a todos los medios de comunicación físicamente controlados, pueden ser explicadas. | Mucho | 1 |
| Los registros de auditoría y de supervisión se examinan rutinariamente para detectar anomalías, y que se tomen medidas correctivas cuando sea necesario. | Mucho | 1 |
| Requisitos de la organización para el seguimiento de la seguridad física se comunicarán formalmente a todos los contratistas y proveedores de servicios que | Mucho | 1 |

| | | |
|---|---|---|
| controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software. | | |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el monitoreo de la seguridad física. | Mucho | 1 |

**Tabla 10. Monitoreo y Auditoría de Seguridad Física (Área 8)**

**Área 9. Gestión de Sistema y Red:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Están documentados y probados los planes de seguridad para la protección de los sistemas y redes. | Nada | 3 |
| La información confidencial está protegida por un almacenamiento seguro (por ejemplo, las copias de seguridad almacenadas fuera del sitio). | Mucho | 1 |
| La integridad del software instalado se verifica regularmente. | Mucho | 1 |
| Todos los sistemas están al día con respecto a las revisiones, parches y recomendaciones en los avisos de seguridad. | Mucho | 1 |
| Hay un plan de copia de seguridad de datos documentados y probados para las copias de | Algo | 2 |

| | | |
|---|---|---|
| seguridad de software y datos. Todo el personal entiende sus responsabilidades en virtud de los planes de copia de seguridad. | | |
| Los cambios en hardware y software son planeados, controlados y documentados. | Algo | 2 |
| Miembros del personal de TI siguen procedimientos al expedir, cambiar, y terminar las contraseñas de los usuarios, las cuentas y privilegios; se requiere una identificación de usuario único para todos los usuarios de sistemas de información, incluidos los usuarios de terceros, cuentas predeterminadas y contraseñas por defecto han sido eliminados de los sistemas. | Mucho | 1 |
| Sólo los servicios necesarios se están ejecutando en los sistemas - todos los servicios innecesarios se han eliminado. | Mucho | 1 |
| Se utilizan herramientas y mecanismos para la seguridad del sistema y administración de la red , y se revisan y actualizan de forma rutinaria o son reemplazados. | Mucho | 1 |
| Los requerimientos de la administración de los sistemas y redes relacionados con la seguridad de la organización son formalmente comunicados a todos los contratistas y proveedores del servicio que mantienen los sistemas y las redes. | Nada | 3 |

| | | |
|---|---|---|
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el sistema relacionado con la seguridad y gestión de red. | Mucho | 1 |

**Tabla 11. Gestión de Sistema y Red (Área 9)**

**Área 10. Monitoreo y Auditoría de Seguridad Informática:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Las herramientas de monitoreo y auditoria de los sistemas y redes son rutinariamente usadas por la organización. Actividad inusual es tratada de acuerdo con la política o procedimiento apropiado. | Algo | 2 |
| Firewall y otros componentes de seguridad son auditados periódicamente por el cumplimiento de las políticas. | Nada | 3 |
| Requisitos de la organización para el seguimiento de la información de seguridad de tecnología se comunicarán formalmente a todos los contratistas y proveedores de servicios que controlan los sistemas y redes. | Algo | 2 |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos | Nada | 3 |

| | | |
|---|---|---|
| para el monitoreo de la seguridad informática. | | |

**Tabla 12. Monitoreo y Auditoría de Seguridad Informática (Área 10)**

**Área 11. Autenticación y Autorización:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Controles adecuados de acceso y autenticación de usuarios (por ejemplo, los permisos de archivos, configuración de red) compatibles con la política se utilizan para restringir el acceso de usuarios a la información, los sistemas sensibles, aplicaciones y servicios específicos, y las conexiones de red. | Algo | 2 |
| Existen políticas y procedimientos para establecer y poner fin al derecho de acceso a la información, tanto para los individuos y grupos documentados. | Algo | 2 |
| Métodos o mecanismos se proporcionan para garantizar que la información sensible no se ha accedido, alterados o destruidos de forma no autorizada. Métodos o mecanismos se revisan y verifican periódicamente. | Mucho | 1 |
| Requisitos de la organización para el control de acceso a los sistemas y la información se comunicarán formalmente a todos los contratistas y proveedores de servicios que | Mucho | 1 |

| | | |
|---|---|---|
| ofrecen servicios de autenticación y autorización. | | |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la autenticación y autorización. | Mucho | 1 |

**Tabla 13. Autenticación y Autorización (Área 11)**

**Área 12. Gestión de Vulnerabilidades:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Hay una serie documentada de procedimientos para la gestión de vulnerabilidades, incluyendo: selección de herramientas de evaluación de vulnerabilidad, listas de comprobación, y escrituras, mantenerse al día con los tipos de vulnerabilidades conocidas y métodos de ataque, revisión de fuentes de información sobre los avisos de vulnerabilidades, alertas de seguridad, y noticias, identificación de los componentes de infraestructura a ser evaluados, programación de las evaluaciones de vulnerabilidad, interpretar y responder a los resultados de la evaluación, mantener un almacenamiento seguro y la disposición de los datos de la vulnerabilidad. | Algo | 2 |

| | | |
|---|---|---|
| Procedimientos de gestión de la vulnerabilidad se siguen y se revisan y actualizan periódicamente. | Algo | 2 |
| Evaluaciones de vulnerabilidad Tecnología se realizan en forma periódica, y las vulnerabilidades se abordan cuando se identifican. | Algo | 2 |
| Requisitos de gestión de la vulnerabilidad de la organización se comunicarán formalmente a todos los contratistas y proveedores de servicios que gestionan las vulnerabilidades tecnológicas. | Algo | 2 |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la gestión de vulnerabilidades. | Algo | 2 |

**Tabla 14. Gestión de Vulnerabilidades (Área 12)**

**Área 13. Cifrado:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Controles de seguridad adecuados se utilizan para proteger la información sensible durante el almacenamiento y durante la transmisión (por ejemplo, el cifrado de datos, infraestructura de clave pública, tecnología de red privada virtual). | Mucho | 1 |

| | | |
|---|---|---|
| Protocolos cifrados se usan cuando los sistemas, enrutadores y servidores de seguridad se manejan de forma remota. | Mucho | 1 |
| Requisitos de la organización para la protección de la información sensible se comunicarán formalmente a todos los contratistas y proveedores de servicios que proporcionan las tecnologías de cifrado. | Nada | 3 |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la aplicación de tecnologías de cifrado. | Algo | 2 |

**Tabla 15. Cifrado (Área 13)**

**Área 14. Diseño y Arquitectura de Seguridad:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| La arquitectura del sistema y el diseño para sistemas nuevos y revisados incluyen consideraciones para: las estrategias de seguridad, políticas y procedimientos, historial de comportamiento de seguridad, los resultados de las evaluaciones de riesgos de seguridad. | Algo | 2 |
| La organización cuenta con los diagramas actualizados que muestran la arquitectura de seguridad de toda la empresa y la topolo- | Algo | 2 |

| | | |
|---|---|---|
| gía de la red. | | |
| Requisitos relacionados con la seguridad de la organización se comunicarán formalmente a todos los contratistas y proveedores de servicios que diseñan sistemas y redes. | Nada | 3 |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la arquitectura y el diseño de la seguridad. | Nada | 3 |

**Tabla 16. Diseño y Arquitectura de Seguridad (Área 14)**

**Área 15. Gestión de Incidentes:**

| **Enunciado** | **¿Hasta qué punto es esta afirmación reflejada en su organización?** | **Puntaje** |
|---|---|---|
| Existen procedimientos documentados para la identificación, notificación y respuesta a incidentes y violaciones de seguridad sospechosos. | Nada | 3 |
| Procedimientos de gestión de incidentes se prueban, verifica y actualiza periódicamente. | Nada | 3 |
| Existen políticas y procedimientos documentados para trabajar con las agencias policiales. | Mucho | 1 |
| Requisitos de la organización para la gestión de incidentes se comunicarán | Nada | 3 |

| | | |
|---|---|---|
| formalmente a todos los contratistas y proveedores de servicios que ofrecen servicios de gestión de incidentes. | | |
| La organización verifica formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la gestión de incidencias. | Nada | 3 |

**Tabla 17. Gestión de Incidentes (Área 15)**

Luego de haber levantado la información, se comienza a detallar cual es el estado del procedimiento de seguridad para dicha área. Para ello, se tomaron tres colores: verde (el cual es un estado bueno), naranja (el cual es un estado regular), y rojo (el cual es un estado malo).

- **Verde**: La organización está llevando a cabo las prácticas de seguridad en el Proceso Inscripciones y Admisiones muy bien; no hay necesidad real para la mejora.
- **Amarillo**: La organización está llevando a cabo las prácticas de seguridad en cierta medida; hay espacio para la mejora.
- **Rojo**: La organización no se está realizando las prácticas de seguridad en el Proceso Inscripciones y Admisiones; existe un amplio margen de mejora.

Para la escogencia del color se basó en lo siguiente:
Por ejemplo, el área 1 tiene 4 características a evaluar. Si cada característica tuviera el mayor valor (el cual es 3=Nada), la suma de todas daría: 3+3+3+3= 12. Si cada característica tuviera el menor valor (el cual es 1=Mucho), la suma de todas daría: 1+1+1+1=4. Por lo tanto para definir la escala de escogencia para esta área, se tomo en cuenta el menor valor que es 4 con el mayor valor que es 12 (es decir el rango [4,5,6,7,8,9,10,11,12]), así que si la suma de todas da 4, 5, o 6, el color asignado seria Verde. Si la suma de todas da 7, 8, o 9, el color asignado seria Amarillo. Pero si la suma de todas da 10, 11, o 12, el color asignado seria Rojo. Esta misma metodología se utilizo para todas las 15 áreas en el momento de asignar el color para las mismas.

Por lo tanto, los resultados para las diferentes 15 áreas fueron las siguientes:

| Área | Color de Estado |
|---|---|
| Área 1. Conciencia y Formación de Seguridad | Amarillo |
| Área 2. Estrategia de Seguridad | Amarillo |
| Área 3. Gestión de la Seguridad | Verde |
| Área 4. Políticas y Reglamentos de Seguridad | Rojo |
| Área 5. Gestión de la Seguridad Colaborativa | Amarillo |
| Área 6. Planes de Contingencia / Recuperación de Desastres | Rojo |
| Área 7. Control de Acceso Físico | Amarillo |
| Área 8. Monitoreo y Auditoría de Seguridad Física | Verde |
| Área 9. Gestión de Sistema y Red | Verde |
| Área 10. Seguimiento y auditoría de Seguridad TI | Rojo |
| Área 11. Autenticación y autorización | Verde |
| Área 12. Gestión de Vulnerabilidades | Amarillo |
| Área 13. Cifrado | Amarillo |
| Área 14. Arquitectura y Diseño de Seguridad | Rojo |
| Área 15. Gestión de Incidentes | Rojo |

**Tabla 18. Color de Estado de cada área**

### 5.4 Selección de Activos Críticos (Paso 5)

Una vez seleccionados todos los activos que hacen parte del proceso Inscripciones y Admisiones, se procede a seleccionar los activos más importantes de dicho proceso.

Para esto, se recurrió a las siguientes preguntas:

Qué activos tendrían un gran impacto negativo en la organización si:

- ¿Estos se dan a conocer a las personas no autorizadas?
- ¿Estos son modificados sin autorización?
- ¿Estos se pierden o se destruyen?
- ¿El acceso a ellos se interrumpe?

Como resultado de esto, surgieron quince activos críticos, los cuales son esenciales en el proceso de Inscripciones y Admisiones. Estos activos son:

- Los servidores que contienen la plataforma para la publicación de las listas
- Base de datos de personas inscritas
- Sistema integrado de recaudo(SQUID)
- Plataforma de inscripciones
- Sistema que realiza la calificación de las tarjetas de respuesta(maquina lectora)
- Formularios
- Tarjetas de respuestas
- Todo el material empacado y sellado en bolsas de seguridad
- Claves de respuesta (respuestas correctas)

- Archivo cifrado del documento que almacena los puntajes de los aspirantes en orden descendentes cargado en SIMCA
- Convenio de cooperación interadministrativo suscrito entre la universidad de Antioquia y la Universidad del Cauca
- Archivos de inscripción
- Credenciales de citación
- Personal de DARCA (Profesional especializado, el universitario)
- Personal de TICS (ingeniero de soporte)

### 5.5 Activos Críticos de Información, Sistemas, Aplicaciones, y Personas (Pasos 6, 7, 8, 9, 10, y 11)

Luego de escoger los activos importantes (críticos), se comenzó a tratar cada activo individualmente, de tal forma que se pudiera levantar más información con respecto al activo crítico y demás activos relacionados con el mismo; se justificó la escogencia de cada activo crítico, se describió el porqué es fundamental para DARCA dicho activo crítico, se observó que activos están relacionados con el activo crítico, se observo si dicho activo cumplía con los requerimientos de seguridad(confidencialidad, integridad y disponibilidad), se anotó que requerimiento de los mencionados anteriormente es más importante para dicho activo, y por último se anotó quien(es) utilizan el activo y quien(es) es el responsable del activo. Se aclara que se centro en los requisitos que deberían ser para el activo del proceso, mas no en los requisitos que actualmente presenta el proceso.

Los resultados son los siguientes:

**Primera parte:**

| **Activo Critico** | **Justificación de selección del activo** | **¿Quien usa el activo?** | **¿Quién es responsable del activo?** |
|---|---|---|---|
| Archivos de inscripción | Estos tienen asociado el tercero al programa y a la prioridad. Sin esta información | División de las tics y DARCA. | División de las tics. |

| | | | |
|---|---|---|---|
| | no se podrían ubicar. | | |
| Credenciales de citación | Contienen la información del sitio, la ubicación y la jornada. Si esto se pierde la gente quedara perdida. | DARCA. | División de las tics es el responsable de generarlas. |
| Formularios | Es la información base para el proceso, si se pierden habrían inconveniente de fraudes. | Solo los aspirantes. | Antes del inicio de la prueba la universidad de Antioquia. Durante la prueba es DARCA, y en adelante también. |
| Tarjetas de respuestas | Es la información base para el proceso, si se pierden habrían inconveniente de fraudes. | Universidad de Antioquia. | Universidad de Antioquia. |
| Material empaca- | Es la infor- | Entidad contratada | Entidad contratada |

| | | | |
|---|---|---|---|
| do y sellado en bolsas de seguridad | mación base para el proceso, si se pierden habrían inconveniente de fraudes. | para el diseño y la aplicación de la prueba de admisión(Universidad de Antioquia) | para el diseño y la aplicación de la prueba de admisión(Universidad de Antioquia) |
| Claves de respuesta (respuestas correctas) | Es la información base para el proceso, si se pierden habrían inconveniente de fraudes y no se podrían calificar. | Entidad contratada para el diseño y la aplicación de la prueba de admisión (universidad de Antioquia), DARCA. | Entidad contratada para el diseño y la aplicación de la prueba de admisión(universidad de Antioquia) |
| Archivo cifrado del documento que almacena los puntajes de los aspirantes. | Es de gran vulnerabilidad ya que se podrían alterar los resultados. | DARCA | TICS |
| Convenio de cooperación interadministrativo suscrito entre la universidad de Antioquia y la | Si falta no se puede llevar a cabo la prueba | Universidad de Antioquia y Universidad del Cauca. | Universidad de Antioquia y Universidad del Cauca. |

| | | | |
|---|---|---|---|
| Universidad del Cauca. | | | |
| Los servidores que contienen la plataforma para la publicación de las listas. | Si se daña se interrumpe el proceso, ya que es el mecanismo que entrega la información a la gente. | TICS | TICS |
| El sistema que realiza la calificación de las tarjetas de respuesta (maquina lectora). | Si este sistema tiene un daño, tienen errores los resultados. | Universidad de Antioquia | Universidad de Antioquia |
| Sistema integrado de recaudo (SQUID). | Si se daña puede llegar a impedir la realización de las inscripciones. | DARCA | TICS |
| Base de datos de personas inscritas. | Es confidencial porque son los datos de terceros. | DARCA | TICS |
| Plataforma de | Si se cae o se daña, los | DARCA | TICS |

| | | | |
|---|---|---|---|
| inscripciones. | terceros no pueden realizar su inscripción. | | |
| Personal de DARCA (Profesional especializado, el universitario). | Tienen información muy importante referente al proceso de inscripciones y admisiones en DARCA. | Sus habilidades son el desarrollo e integración de los procesos y procedimientos, y la normatividad institucional. | |
| Personal de TICS (ingeniero de soporte). | Tienen información muy importante referente al proceso de inscripciones y admisiones en DARCA. | Sus habilidades son el desarrollo. | |

**Tabla 19. Información de Activos Críticos (Primera Parte)**

**Segunda Parte:**

| **Activo Critico** | **Activos Relacionados** | **Requisitos de Seguridad** | **Requisitos de Seguridad más Importante** |
|---|---|---|---|
| Archivos de ins- | Sistemas: Servi- | Confidencialidad, | Integridad |

| | | | |
|---|---|---|---|
| cripción | dores.<br><br>Aplicaciones: SIMCA. | Integridad, Disponibilidad. | |
| Credenciales de citación | Sistemas: Servidores.<br><br>Aplicaciones: SIMCA. | Confidencialidad, Integridad, Disponibilidad. | Integridad |
| Formularios | Ninguno. | Confidencialidad, Integridad, Disponibilidad. | Confidencialidad |
| Tarjetas de respuestas | Sistemas: dispositivo de lectura, servidor que guarda la información de la lectura de las hojas de tarjetas de respuesta.<br><br>Aplicaciones: software de calificación. | Confidencialidad, Integridad, Disponibilidad. | Integridad |
| Material empacado y sellado en bolsas de seguridad | Transporte o la cadena de custodia. | Confidencialidad, Integridad, Disponibilidad. | Integridad |
| Claves de respuesta (respuestas correc- | Ninguno. | Confidencialidad, Integridad, Dis- | Confidencialidad |

| | | | |
|---|---|---|---|
| tas) | | ponibilidad. | |
| Archivo cifrado del documento que almacena los puntajes de los aspirantes. | Sistemas: Servidores.<br>Aplicaciones: SIMCA. | Confidencialidad, Integridad, Disponibilidad. | Integridad |
| Convenio de cooperación interadministrativo suscrito entre la universidad de Antioquia y la Universidad del Cauca. | Ninguno. | Integridad, Disponibilidad. | Integridad |
| Los servidores que contienen la plataforma para la publicación de las listas. | Ninguno. | Confidencialidad, Integridad, Disponibilidad. | Integridad |
| El sistema que realiza la calificación de las tarjetas de respuesta (maquina lectora). | Ninguno. | Integridad, Disponibilidad. | Integridad |
| Sistema integrado de recaudo (SQUID). | Sistemas: Servidores. | Confidencialidad, Integridad, Disponibilidad. | Disponibilidad |

| | | | |
|---|---|---|---|
| Base de datos de personas inscritas. | Sistemas: Servidores. | Confidencialidad, Integridad, Disponibilidad. | Confidencialidad |
| Plataforma de inscripciones. | Sistemas: Servidores. | Confidencialidad, Integridad, Disponibilidad. | Disponibilidad |
| Personal de DARCA (Profesional especializado, el universitario). | Aplicaciones: SIMCA (plataforma administrativa).<br><br>Información: convenio, y el desarrollo de los procesos y procedimiento de la contraparte y lo demás que usen. | Disponibilidad | Disponibilidad |
| Personal de TICS (ingeniero de soporte). | Sistemas: servidores e información almacenada.<br><br>Aplicaciones: bases de datos, SIMCA, SQUID, correo electrónico institucional. | Disponibilidad | Disponibilidad |

**Tabla 20. Información de Activos Críticos (Segunda Parte)**

Siler Amador Donado
D.N.I 72.168.640

### 5.6 Perfil de riesgo de Información – Perfil de riesgo básico (Paso 12)

En este paso se procede a determinar si existen o podrían existir en un futuro posibles amenazas para un activo. Entonces se manejan varios criterios de amenaza:

- Tipo de Acceso: El tipo de acceso al activo podría ser por medio de la red, o por medio físico.

- Tipo de Actor: El tipo de actor podría ser interno a DARCA (funcionario), o externo a DARCA (un tercero).

- Motivo: El motivo del ataque o amenaza podría ser accidental o deliberada.

- Resultado: Los resultados que podría provocar la amenaza si resulta exitosa son: revelación, modificación, pérdida/destrucción, interrupción.

Los resultados son los siguientes:

| **Activo** | **Tipo de Acceso** | **Tipo de Actor** | **Motivo** | **Resultado** |
|---|---|---|---|---|
| Archivos de inscripción | Red | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi- perdida/destrucción, interrupción. |
| Credenciales de citación | Red | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi- perdida/destrucción, |

| | | | | |
|---|---|---|---|---|
| | | | | interrupción. |
| Formularios | Físico | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi-perdida/destrucción, interrupción. |
| Tarjetas de respuestas | Físico | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi-perdida/destrucción, interrupción. |
| Material empacado y sellado en bolsas de seguridad | Físico | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi-perdida/destrucción, interrupción. |
| Claves de respuesta (respuestas correctas) | Red | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi-perdida/destrucción, interrupción. |
| Archivo cifrado del documento que almacena los puntajes de los aspirantes. | Red | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi-perdida/destrucción, interrupción. |
| Convenio de | Físico | Dentro, fuera. | Accidental, | Revelación, modifi- |

| | | | | |
|---|---|---|---|---|
| cooperación interadministrativo suscrito entre la universidad de Antioquia y la Universidad del Cauca. | | | Deliberado. | cación, perdida/destrucción, interrupción. |
| Los servidores que contienen la plataforma para la publicación de las listas. | Red, Físico. | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi- perdida/destrucción, interrupción. |
| El sistema que realiza la calificación de las tarjetas de respuesta (maquina lectora). | Físico | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi- perdida/destrucción, interrupción. |
| Sistema integrado de recaudo (SQUID). | Red | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi- perdida/destrucción, interrupción. |
| Base de datos de personas inscritas. | Red | Dentro, fuera. | Accidental, Deliberado. | Revelación, modificación, perdi- perdida/destrucción, interrupción. |

| | | | | |
|---|---|---|---|---|
| Plataforma de inscripciones. | Red | Dentro, fuera. | | Revelación, modificación, perdi- perdida/destrucción, interrupción. |
| Personal de DARCA (Profesional especializado, el universitario). | No aplica | Tomar permiso de ausencia temporal (debido a una enfermedad, discapacidad), dejar DARCA de forma permanente (jubilación), amenazas que afecten a un tercero o proveedor de servicios. | No aplica | Revelación, modificación, perdi- perdida/destrucción, interrupción. |
| Personal de TICS (ingeniero de soporte). | No aplica | Tomar permiso de ausencia temporal (debido a una enfermedad, discapaci- | No aplica | Revelación, modificación, perdi- perdida/destrucción, interrupción. |

| | | | | |
|---|---|---|---|---|
| | | dad), dejar DARCA de forma permanente (jubilación), amenazas que afecten a un tercero o proveedor de servicios. | | |

**Tabla 21. Perfil de riesgo Básico**

### 5.7 Perfil de riesgo de Información - Contexto de la amenaza (Pasos 13, 14, 15)

El objetivo en el paso 13 fue encontrar los actores que plantean las mayores amenazas al activo crítico a través del acceso a la red y a través del acceso físico.

En el paso 14, el objetivo fue analizar qué tan fuerte era el motivo de los actores (definidos en el paso anterior) para plantear amenazas a los activos. Se evaluó como alto, medio, bajo.

El objetivo en el paso 15 fue encontrar con qué frecuencia han ocurrido las amenazas (descubiertas en el paso 12) en el pasado. Para este paso fue esencial leer sobre algunos datos históricos de DARCA.

Los resultados son los siguientes (acceso a través de la red):

| **Activo Critico** | **¿Qué actores plantean las mayores amenazas a esta información a través de la red?** | **¿Qué tan fuerte es el motivo del actor?** | **¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?** |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| Archivo cifrado del documento que almacena los puntajes de los aspirantes. | Funcionarios de DARCA con privilegios. | alto | 0 veces en 2 años |
| Archivos de inscripción | Funcionarios de DARCA utilizando la plataforma administrativa que permite modificar datos de inscripción. Las tics cuando administran la base de datos. UDEA accidentalmente podría modificar los archivos de inscripción al manipularlos. | medio | 0 veces en 2 años |
| Credenciales de citación | Personal de tics, UDEA. | alto | 0 veces en 2 años |
| Los servidores que contienen la plataforma para la publicación de las listas. | Personal de servidores, TICS, Agente externo (Ataque DOS) | alto | 0 veces en 3 años |
| Sistema integrado | TICS, División | Alto | 0 veces en 3 años |

| | | | |
|---|---|---|---|
| de recaudo (SQUID). | Financiera, Administrador de Base de Datos, Entidades de recaudo. | | |
| Base de datos de personas inscritas. | Administrador de Base de datos, DARCA, TICS, UDEA. | Alto | 0 veces en 3 años |
| Plataforma de inscripciones. | TICS, agente externo (ataque DOS). | Alto | 0 veces en 3 años |

**Tabla 22. Contexto de la Amenaza (Acceso a través de la red)**

Los resultados son los siguientes (acceso físico):

| **Activo Critico** | **¿Qué actores plantean las mayores amenazas a esta información a través de medios físicos?** | **¿Qué tan fuerte es el motivo del actor?** | **¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?** |
|---|---|---|---|
| Los servidores que contienen la plataforma para la publicación de las listas. | Personal de servidores. | Alto | 0 veces en 3 años |
| El sistema que realiza la calificación de las tarjetas | UDEA | Alto | 0 veces en 2 años |

| | | | |
|---|---|---|---|
| de respuesta (maquina lectora). | | | |
| Convenio de cooperación interadministrativo suscrito entre la universidad de Antioquia y la Universidad del Cauca. | Personal de DARCA que gestiona el documento, personal perteneciente a la entidad contratada | Bajo | 0 veces en 2 años |
| Formularios | UDEA, empresa trasportadora. | Bajo | 0 veces en 2 años |
| Tarjetas de respuestas | Agente externo que quiera pasar ilícitamente a la Unicauca. | Alto | 0 veces en 2 años |
| Material empacado y sellado en bolsas de seguridad | Personal que tiene a cargo el material (ya se ha presentado la prueba), personal de la entidad contratada (antes de que se procese el material). | Alto | 0 veces en 2 años |
| Claves de respuesta (respuestas correc- | No hay. | bajo | 0 veces en 2 años |

| | | | |
|---|---|---|---|
| tas) | | | |

**Tabla 23. Contexto de la Amenaza (Acceso Físico)**

### 5.8 Perfil de riesgo de Información - Áreas de preocupación (Paso 16)

En esta parte se construyeron ejemplos de cómo los actores tanto internos como externos, y bien sea deliberada o accidentalmente podrían amenazar el activo crítico por medio de la red o físicamente. Esto con el fin de tener una idea de las diferentes amenazas que podrían surgir en el proceso de Inscripciones y Admisiones.

### 5.9 Rutas de acceso a la Red (Pasos 17 y 18)

En estos pasos se procede a levantar la información del sistema o los sistemas que están estrechamente relacionados con el activo crítico, esto con el fin de ver si existen rutas de acceso por medio de la red para acceder al activo crítico. Un ejemplo de estos sistemas es:

- El sistema en el que el activo crítico reside
- El sistema a donde se iría para obtener una copia oficial del activo crítico
- El sistema que ofrece a los usuarios legítimos el acceso a un activo crítico
- El sistema que le da un acceso al actor de amenaza a un activo crítico

Luego de hallar los sistemas de interés se procede a analizar qué clases de componentes son parte del sistema de interés, que clases de componentes se utilizan para transmitir información y aplicaciones desde el sistema de interés para la gente, que clases de componentes pueden las personas (por ejemplo, los usuarios, los atacantes) usar para acceder al sistema de interés, y en qué clase de componentes está la información del sistema de interés almacenados como copia de seguridad. Un ejemplo de estas clases de componentes son los servidores, redes internas/externas, sede de estaciones de trabajo, laptops, PDAs/Componentes inalámbricos, Hogar/Estaciones de trabajo externos, Dispositivos de almacenamiento, etc.

| **Activo** | **Sistema o sistemas que están relacionados con el activo crítico.** | **Clases de componentes que son parte del sistema de interés.** | **Clases de componentes que se utilizan para transmitir información y aplicaciones desde el sistema de interés para la gente.** | **Clases de componentes desde donde las personas (los usuarios, los atacantes) pueden acceder al sistema de intereses** | **Clase de componentes en donde la información del sistema de interés está almacenada como copia de seguridad.** |
|---|---|---|---|---|---|
| Archivo cifrado que almacena los puntajes | SIMCA, el sistema que lo cifra. | Servidores, redes internas, computadores. | Redes externas | Sede de estaciones de trabajo | Dispositivos de almacenamiento. |
| Archivos de Inscripción | SIMCA, SQUID. | Servidores, redes internas, estaciones de trabajo. | Redes externas | Portátiles, PDAs/ componentes inalámbricos. | Dispositivos de almacenamiento. |
| Credenciales de citación. | SIMCA | Servidores, redes internas. | Redes externas. | Sede de estaciones de trabajo (redes internas). | Dispositivos de almacenamiento |

| | | | | | |
|---|---|---|---|---|---|
| Los servidores que contienen la plataforma para la publicación de las listas. | Plataforma para publicación de las listas | Redes internas | Redes externas. | Portátiles, PDAs/ componentes inalámbricos. | Ninguno |
| Sistema integrado de recaudo (SQUID). | SIMCA | Servidores, redes internas. | Redes externas. | Portátiles, PDAs/ componentes inalámbricos. | Ninguno |
| Base de datos de personas inscritas. | servidor | Servidores, redes internas. | Redes externas. | Portátiles, PDAs/ componentes inalámbricos. | Dispositivos de almacenamiento |
| Plataforma de inscripciones. | servidor | Servidores, redes internas. | Redes externas. | Portátiles, PDAs/ componentes inalámbricos. | Ninguno |

**Tabla 24. Rutas de Acceso a la Red**

### 5.10 Revisión de la infraestructura (Pasos 19, 20, y 21)

Luego de haber encontrado todos los sistemas y/o clase de componentes que están muy relacionados con los activos críticos, se procede a determinar quien o

quienes son los responsables de mantener y asegurar cada sistema y/o clase de componente. También se determinó hasta qué punto se considera la seguridad durante la configuración y mantenimiento de cada clase de componente y/o sistema, tomando como referencia las variables “Mucho”, “Algo”, “Nada”, “No se sabe”.

| **Clase de componentes** | **Activos críticos relacionados** | **Responsables de mantener y asegurar cada clase de componente** | **Grado de seguridad durante la configuración y mantenimiento de cada clase de componentes.** |
|---|---|---|---|
| Servidores Específicos | Archivo cifrado del documento que almacena los puntajes, Archivos de Inscripción, Credenciales de citación, Servidores que contienen la plataforma para la publicación de las listas, Base de datos de personas inscritas, Plataforma de inscripciones, Sistema integrado de recaudo (SQUID). | DBA(tics) | No se sabe. |
| Oficina de | Archivo cifrado del | Profesional | Mucho. |

| | | | |
|---|---|---|---|
| admisiones | documento que almacena los puntajes, Servidores que contienen la plataforma para la publicación de las listas, Plataforma de inscripciones, Sistema integrado de recaudo (SQUID). | especializado | |
| Oficina de SIMCA | Archivo cifrado del documento que almacena los puntajes, Servidores que contienen la plataforma para la publicación de las listas, Plataforma de inscripciones. | Coordinador. | Mucho. |
| Oficina de sistemas TICS | Archivos de Inscripción, Credenciales de citación, Servidores que contienen la plataforma para la publicación de las listas, Base de datos de personas inscritas, Plataforma de inscripciones. | Personal asignado a la labor. | Mucho. |

| | | | |
|---|---|---|---|
| Oficina financiera | Sistema integrado de recaudo (SQUID). | Personal asignado a la labor. | Mucho. |

**Tabla 25. Revisión de la Infraestructura**

### 5.11 Perfil de riesgo de Información - Impacto potencial de amenazas (Paso 22)

En este paso se procede a medir el impacto potencial al ocurrir amenazas (descritas en el paso 12) en cada sector de aplicación (reputación, finanzas, productividad, seguridad/salud) en DARCA. Se evaluó mediante las medidas bajo, medio, y alto en la parte cualitativa, y 1, 2, y 3 en la parte cuantitativa (respectivamente). Lo anterior se midió con respecto al paso doce, en donde se señalan las posibles amenazas al activo crítico que se podrían presentar en algún momento. Por ejemplo si existe una persona que por medio de la red accede al activo crítico accidentalmente y provocó una pérdida de este, el impacto que ocasiona en el sector de productividad es alto. Esto se hizo para todos los quince activos críticos.

Para el activo **Archivo cifrado del documento que almacena los puntajes:**

| Tipo de Acceso | Actor | Motivo | Resultado | Reputación | Financiero | Productividad | Seguridad | Puntaje |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | A | B | B | B | 6 |
| Red | Interno | Accidental | Modificación | A | B | B | B | 6 |
| Red | Interno | Accidental | Perdida/Destrucción | A | B | B | B | 6 |
| Red | Interno | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Interno | Deliberado | Revelación | A | B | M | B | 7 |
| Red | Interno | Deliberado | Modificación | A | B | M | B | 7 |
| Red | Interno | Deliberado | Perdida/Destrucción | A | B | A | B | 8 |
| Red | Interno | Deliberado | Interrupción | A | B | M | B | 7 |
| Red | Externo | Accidental | Revelación | A | B | B | B | 6 |
| Red | Externo | Accidental | Modificación | A | B | B | B | 6 |
| Red | Externo | Accidental | Perdida/Destrucción | A | B | B | B | 6 |
| Red | Externo | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Externo | Deliberado | Revelación | A | B | B | B | 6 |
| Red | Externo | Deliberado | Modificación | A | B | B | B | 6 |
| Red | Externo | Deliberado | Perdida/Destrucción | A | A | B | B | 8 |
| Red | Externo | Deliberado | Interrupción | A | B | B | B | 6 |

Siler Amador Donado
D.N.I 72.168.640

**Tabla 26. Impacto potencial de amenazas Archivo cifrado del documento que almacena los puntajes**

Para el activo **Archivos de inscripción:**

| Tipo de Acceso | Actor | Motivo | Resultado | Reputación | Financiero | Productividad | Seguridad | Puntaje |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | A | B | B | B | 6 |
| Red | Interno | Accidental | Modificación | A | B | B | B | 6 |
| Red | Interno | Accidental | Perdida/Destrucción | A | A | B | B | 8 |
| Red | Interno | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Interno | Deliberado | Revelación | A | B | B | B | 6 |
| Red | Interno | Deliberado | Modificación | A | B | B | B | 6 |
| Red | Interno | Deliberado | Perdida/Destrucción | A | A | B | B | 8 |
| Red | Interno | Deliberado | Interrupción | A | B | M | B | 7 |
| Red | Externo | Accidental | Revelación | A | B | B | B | 6 |
| Red | Externo | Accidental | Modificación | A | B | B | B | 6 |
| Red | Externo | Accidental | Perdida/Destrucción | A | A | B | B | 8 |
| Red | Externo | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Externo | Deliberado | Revelación | A | A | B | B | 8 |
| Red | Externo | Deliberado | Modificación | A | B | M | B | 7 |
| Red | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Externo | Deliberado | Interrupción | A | B | B | B | 6 |

**Tabla 27. Impacto potencial de amenazas Archivos de inscripción**

Para el activo **Claves de respuestas:**

| Tipo de Acceso | Actor | Motivo | Resultado | Reputación | Financiero | Productividad | Seguridad | Puntaje |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Red | Interno | Accidental | Modificación | B | B | B | B | 4 |
| Red | Interno | Accidental | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Interno | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Modificación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Interno | Deliberado | Interrupción | B | B | B | B | 4 |
| Red | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Red | Externo | Accidental | Modificación | B | B | B | B | 4 |
| Red | Externo | Accidental | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Externo | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Modificación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Externo | Deliberado | Interrupción | B | B | B | B | 4 |

**Tabla 28. Impacto potencial de amenazas Claves de respuesta**

Para el activo **Convenio de cooperación interadministrativo:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Físico | Interno | Accidental | Modificación | B | B | B | B | 4 |
| Físico | Interno | Accidental | Perdida/Destrucción | B | B | B | B | 4 |
| Físico | Interno | Accidental | Interrupción | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Físico | Interno | Deliberado | Modificación | B | B | B | B | 4 |
| Físico | Interno | Deliberado | Perdida/Destrucción | B | B | B | B | 4 |
| Físico | Interno | Deliberado | Interrupción | A | A | A | B | 10 |
| Físico | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Físico | Externo | Accidental | Modificación | B | B | B | B | 4 |
| Físico | Externo | Accidental | Perdida/Destrucción | B | B | B | B | 4 |
| Físico | Externo | Accidental | Interrupción | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Modificación | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Perdida/Destrucción | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Interrupción | A | A | A | B | 10 |

**Tabla 29. Impacto potencial de amenazas Convenio de cooperación interadministrativo**

Para el activo **Credenciales de citación:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Red | Interno | Accidental | Modificación | A | B | M | B | 7 |
| Red | Interno | Accidental | Perdida/Destrucción | A | B | M | B | 7 |
| Red | Interno | Accidental | Interrupción | M | B | M | B | 6 |
| Red | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Modificación | A | B | M | B | 7 |
| Red | Interno | Deliberado | Perdida/Destrucción | A | B | M | B | 7 |
| Red | Interno | Deliberado | Interrupción | M | B | M | B | 6 |
| Red | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Red | Externo | Accidental | Modificación | A | B | M | B | 7 |
| Red | Externo | Accidental | Perdida/Destrucción | A | B | M | B | 7 |
| Red | Externo | Accidental | Interrupción | M | B | M | B | 6 |
| Red | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Modificación | A | B | M | B | 7 |
| Red | Externo | Deliberado | Perdida/Destrucción | A | B | M | B | 7 |
| Red | Externo | Deliberado | Interrupción | M | B | M | B | 6 |

**Tabla 30. Impacto potencial de amenazas Credenciales de citación**

Para el activo **Formularios:**

Siler Amador Donado
D.N.I 72.168.640

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | A | A | A | B | 10 |
| Físico | Interno | Accidental | Modificación | A | A | A | B | 10 |
| Físico | Interno | Accidental | Perdida/Destrucción | B | B | A | B | 6 |
| Físico | Interno | Accidental | Interrupción | B | B | A | B | 6 |
| Físico | Interno | Deliberado | Revelación | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Modificación | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Perdida/Destrucción | B | B | A | B | 6 |
| Físico | Interno | Deliberado | Interrupción | B | B | A | B | 6 |
| Físico | Externo | Accidental | Revelación | A | A | A | B | 10 |
| Físico | Externo | Accidental | Modificación | A | A | A | B | 10 |
| Físico | Externo | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Accidental | Interrupción | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Revelación | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Modificación | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Interrupción | B | B | B | B | 4 |

**Tabla 31. Impacto potencial de amenazas Formularios**

Para el activo **Material empacado y sellado en bolsas de seguridad:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | B | A | B | B | 6 |
| Físico | Interno | Accidental | Modificación | A | A | A | B | 10 |
| Físico | Interno | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Interno | Accidental | Interrupción | M | M | M | B | 7 |
| Físico | Interno | Deliberado | Revelación | B | A | B | B | 6 |
| Físico | Interno | Deliberado | Modificación | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Interrupción | M | M | M | B | 7 |
| Físico | Externo | Accidental | Revelación | B | A | B | B | 6 |
| Físico | Externo | Accidental | Modificación | A | A | A | B | 10 |
| Físico | Externo | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Accidental | Interrupción | M | M | M | B | 7 |
| Físico | Externo | Deliberado | Revelación | B | A | B | B | 6 |
| Físico | Externo | Deliberado | Modificación | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Interrupción | M | M | M | B | 7 |

**Tabla 32. Impacto potencial de amenazas Material empacado y sella-do en bolsas de seguridad**

Para el activo **Tarjetas de Respuesta Diligenciadas:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | A | A | B | B | 8 |
| Físico | Interno | Accidental | Modificación | A | A | A | B | 10 |
| Físico | Interno | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Interno | Accidental | Interrupción | B | B | B | B | 4 |
| Físico | Interno | Deliberado | Revelación | A | A | B | B | 8 |
| Físico | Interno | Deliberado | Modificación | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Interrupción | B | B | B | B | 4 |
| Físico | Externo | Accidental | Revelación | A | A | B | B | 8 |
| Físico | Externo | Accidental | Modificación | A | A | A | B | 10 |
| Físico | Externo | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Accidental | Interrupción | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Revelación | A | A | B | B | 8 |
| Físico | Externo | Deliberado | Modificación | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Interrupción | B | B | B | B | 4 |

**Tabla 33. Impacto potencial de amenazas Tarjetas de Respuesta Diligenciadas**

Para el activo **Servidores que contienen la plataforma para la publicación de las listas (red y físico):**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Red | Interno | Accidental | Modificación | A | A | M | B | 9 |
| Red | Interno | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Interno | Accidental | Interrupción | A | M | M | B | 8 |
| Red | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Modificación | A | A | M | B | 9 |
| Red | Interno | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Interno | Deliberado | Interrupción | A | M | M | B | 8 |
| Red | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Red | Externo | Accidental | Modificación | A | A | M | B | 9 |
| Red | Externo | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Externo | Accidental | Interrupción | A | M | M | B | 8 |
| Red | Externo | Deliberado | Revelación | B | B | B | B | 4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Red | Externo | Deliberado | Modificación | A | A | M | B | 9 |
| Red | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Externo | Deliberado | Interrupción | A | M | M | B | 8 |

**Tabla 34. Impacto potencial de amenazas Servidores que contienen la plataforma para la publicación de las listas (red)**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Físico | Interno | Accidental | Modificación | A | A | M | B | 9 |
| Físico | Interno | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Interno | Accidental | Interrupción | A | M | M | B | 8 |
| Físico | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Físico | Interno | Deliberado | Modificación | A | A | M | B | 9 |
| Físico | Interno | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Interno | Deliberado | Interrupción | A | M | M | B | 8 |
| Físico | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Físico | Externo | Accidental | Modificación | A | A | M | B | 9 |
| Físico | Externo | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Accidental | Interrupción | A | M | M | B | 8 |
| Físico | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Modificación | A | A | M | B | 9 |
| Físico | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Físico | Externo | Deliberado | Interrupción | A | M | M | B | 8 |

**Tabla 35. Impacto potencial de amenazas Servidores que contienen la plataforma para la publicación de las listas (físico)**

Para el activo **Sistema que realiza la calificación de las tarjetas de respuesta (maquina lectora):**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Físico | Interno | Accidental | Modificación | B | B | A | B | 6 |
| Físico | Interno | Accidental | Perdida/Destrucción | B | A | A | B | 8 |
| Físico | Interno | Accidental | Interrupción | M | B | M | B | 6 |
| Físico | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Físico | Interno | Deliberado | Modificación | B | B | A | B | 6 |
| Físico | Interno | Deliberado | Perdida/Destrucción | B | A | A | B | 8 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Físico | Interno | Deliberado | Interrupción | M | B | M | B | 6 |
| Físico | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Físico | Externo | Accidental | Modificación | B | B | A | B | 6 |
| Físico | Externo | Accidental | Perdida/Destrucción | B | A | A | B | 8 |
| Físico | Externo | Accidental | Interrupción | M | B | M | B | 6 |
| Físico | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Físico | Externo | Deliberado | Modificación | B | B | A | B | 6 |
| Físico | Externo | Deliberado | Perdida/Destrucción | B | A | A | B | 8 |
| Físico | Externo | Deliberado | Interrupción | M | B | M | B | 6 |

**Tabla 36. Impacto potencial de amenazasSistema que realiza la calificación de las tarjetas de respuesta (maquina lectora)**

Para el activo **Base de datos de personas inscritas:**

| **Tipo de Acceso** | **Actor** | **Motivo** | **Resultado** | **Reputación** | **Financiero** | **Productividad** | **Seguridad** | **Puntaje** |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Red | Interno | Accidental | Modificación | A | A | A | B | 10 |
| Red | Interno | Accidental | Perdida/Destrucción | A | M | A | B | 9 |
| Red | Interno | Accidental | Interrupción | M | M | M | B | 7 |
| Red | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Modificación | A | A | A | B | 10 |
| Red | Interno | Deliberado | Perdida/Destrucción | A | M | A | B | 9 |
| Red | Interno | Deliberado | Interrupción | M | M | M | B | 7 |
| Red | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Red | Externo | Accidental | Modificación | A | A | A | B | 10 |
| Red | Externo | Accidental | Perdida/Destrucción | A | M | A | B | 9 |
| Red | Externo | Accidental | Interrupción | M | M | M | B | 7 |
| Red | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Modificación | A | A | A | B | 10 |
| Red | Externo | Deliberado | Perdida/Destrucción | A | M | A | B | 9 |
| Red | Externo | Deliberado | Interrupción | M | M | M | B | 7 |

**Tabla 37. Impacto potencial de amenazas Base de datos de personas inscritas**

Para el activo **Plataforma de inscripciones:**

| **Tipo de Acceso** | **Actor** | **Motivo** | **Resultado** | **Reputación** | **Financiero** | **Productividad** | **Seguridad** | **Puntaje** |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Red | Interno | Accidental | Modificación | A | A | A | B | 10 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Interno | Accidental | Interrupción | A | B | A | B | 8 |
| Red | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Modificación | A | A | A | B | 10 |
| Red | Interno | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Interno | Deliberado | Interrupción | A | B | A | B | 8 |
| Red | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Red | Externo | Accidental | Modificación | A | A | A | B | 10 |
| Red | Externo | Accidental | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Externo | Accidental | Interrupción | A | B | A | B | 8 |
| Red | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Modificación | A | A | A | B | 10 |
| Red | Externo | Deliberado | Perdida/Destrucción | A | A | A | B | 10 |
| Red | Externo | Deliberado | Interrupción | A | B | A | B | 8 |

**Tabla 38. Impacto potencial de amenazas Plataforma de inscripciones**

Para el activo **Sistema integrado de recaudo (SQUID):**

| **Tipo de Acceso** | **Actor** | **Motivo** | **Resultado** | **Reputación** | **Financiero** | **Productividad** | **Seguridad** | **Puntaje** |
|---|---|---|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | B | B | B | 4 |
| Red | Interno | Accidental | Modificación | B | B | B | B | 4 |
| Red | Interno | Accidental | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Interno | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Interno | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Modificación | B | B | B | B | 4 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Interno | Deliberado | Interrupción | B | B | B | B | 4 |
| Red | Externo | Accidental | Revelación | B | B | B | B | 4 |
| Red | Externo | Accidental | Modificación | B | B | B | B | 4 |
| Red | Externo | Accidental | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Externo | Accidental | Interrupción | B | B | B | B | 4 |
| Red | Externo | Deliberado | Revelación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Modificación | B | B | B | B | 4 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | B | B | B | 4 |
| Red | Externo | Deliberado | Interrupción | B | B | B | B | 4 |

**Tabla 39. Impacto potencial Sistema integrado de recaudo (SQUID)**

Para el activo **Personal de DARCA (Profesional especializado, el universitario):**

| Actor | Motivo | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|
| personas clave que toman un permiso de ausencia tempo-ral(por ejemplo, debido a una enfermedad, discapacidad) | Revelación | B | B | B | B | 4 |
| | Modificación | B | B | B | B | 4 |
| | Perdida/Destrucción | B | B | B | B | 4 |
| | Interrupción | B | B | B | B | 4 |
| personas clave que dejan la organización de forma permanen-te (por ejemplo, jubilación, otras oportunidades) | Revelación | B | B | B | B | 4 |
| | Modificación | B | B | B | B | 4 |
| | Perdida/Destrucción | B | B | B | B | 4 |
| | Interrupción | B | B | B | B | 4 |
| amenazas que afectan a un terce-ro o proveedor de servicios | Revelación | B | B | B | B | 4 |
| | Modificación | A | B | B | B | 6 |
| | Perdida/Destrucción | A | A | A | B | 10 |
| | Interrupción | A | B | M | B | 7 |

**Tabla 40. Impacto potencial de amenazas Personal de DARCA (Profe-sional especializado, el universitario)**

Para el activo **Personal de TICS (ingeniero de soporte):**

| Actor | Motivo | Repu-tación | Finan ciero | Produc tividad | Seguri dad | Punta-je |
|---|---|---|---|---|---|---|
| personas clave que toman un permiso de ausencia tempo-ral(por ejemplo, debido a una enfermedad, discapacidad) | Revelación | B | B | B | B | 4 |
| | Modificación | B | B | B | B | 4 |
| | Perdida/Destrucción | B | B | B | B | 4 |
| | Interrupción | B | B | B | B | 4 |
| personas clave que dejan la organización de forma permanen-te (por ejemplo, jubilación, otras oportunidades) | Revelación | B | B | B | B | 4 |
| | Modificación | B | B | B | B | 4 |
| | Perdida/Destrucción | B | B | B | B | 4 |
| | Interrupción | B | B | B | B | 4 |
| amenazas que afectan a un terce-ro o proveedor de servicios | Revelación | B | B | B | B | 4 |
| | Modificación | A | B | B | B | 6 |
| | Perdida/Destrucción | A | A | A | B | 10 |
| | Interrupción | A | B | M | B | 7 |

**Tabla 41. Impacto potencial de amenazas Personal de TICS (ingenie-ro de soporte)**

### 5.12 Criterios de Evaluación de Probabilidad (paso 23)

En este paso se definieron las medidas de probabilidad basados en que tan frecuente pueden ocurrir las amenazas para un activo crítico. Para ello se retomó

los tipos de amenazas a los activos críticos y la frecuencia con que cada amenaza en el pasado ocurría. Como resultado de esto se determinó la frecuencia con la que debe producirse una amenaza para ser considerada una amenaza de alta, media, o baja probabilidad.

| Tiempo entre eventos | Frecuencia Anual | Criterio |
|---|---|---|
| Diario | 365 | Alto |
| Semanal | 52 | |
| Mensual | 12 | |
| Cuatro veces al año | 4 | |
| Dos veces al año | 2 | |
| Una vez al año | 1 | Medio |
| Una vez cada 2 años | 0.5 | Bajo |
| Una vez cada 5 años | 0.2 | |
| Una vez cada 10 años | 0.1 | |
| Una vez cada 20 años | 0.05 | |
| Una vez cada 50 años | 0.02 | |

**Tabla 42. Criterios de Evaluación de Probabilidad**

### 5.13 Perfil de riesgo de Información - Probabilidad de ocurrencia de amenazas (Paso 24)

En este paso se procede a determinar qué tan probable es que se produzca la amenaza en el futuro, en donde nos referimos a las amenazas detectadas en el paso 12. Para evaluar dicha probabilidad se basó en la información contextual acerca de los actores de amenaza (paso 13), el motivo de acciones deliberadas por parte de actores humanos (paso 14), la historia de cada amenaza a los activos (paso 15), las áreas de preocupación (paso 16), y los criterios de evaluación de probabilidad (paso 23). Las medidas que se tuvieron en cuenta para medir la probabilidad son alto, medio y bajo para la parte cualitativa, y 3, 2, 1 para la parte cuantitativa (respectivamente).

Para el activo **Archivo cifrado del documento que almacena los puntajes:**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 43. Probabilidad Archivo cifrado del documento que almacena los puntajes**

Para el activo **Archivos de inscripción:**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 44. Probabilidad Archivos de inscripción**

Para el activo **Claves de respuestas:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Proba-bilidad | Punta-je |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 45. Probabilidad Claves de respuestas**

Para el activo **Convenio de cooperación interadministrativo:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Proba-bilidad | Punta-je |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 46. Probabilidad Convenio de cooperación interadministrativo**

Para el activo **Credenciales de citación:**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 47. Probabilidad Credenciales de citación**

Para el activo **Formularios:**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 48. Probabilidad Formularios**

Para el activo **Material empacado y sellado en bolsas de seguridad:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Proba-bilidad | Punta-je |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 3 |
| Red | Interno | Deliberado | Modificación | B | 3 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 3 |
| Red | Interno | Deliberado | Interrupción | B | 3 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 49. Probabilidad Material empacado y sellado en bolsas de seguridad**

Para el activo **Tarjetas de Respuesta Diligenciadas:**

| Tipo de Acceso | Actor | Motivo | Resul-tado | Proba bilidad | Punta-je |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 1 |
| Red | Interno | Deliberado | Modificación | B | 1 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Interno | Deliberado | Interrupción | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 50. Probabilidad Tarjetas de Respuesta Diligenciadas**

Para el activo **Servidores que contienen la plataforma para la publicación de las listas:**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 3 |
| Red | Interno | Deliberado | Modificación | B | 3 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 3 |
| Red | Interno | Deliberado | Interrupción | B | 3 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 3 |
| Red | Externo | Deliberado | Modificación | B | 3 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 3 |
| Red | Ex- | Delibera- | Interrupción | B | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | terno | do | | | |

**Tabla 51. Probabilidad Servidores que contienen la plataforma para la publicación de las listas (red)**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Físico | Interno | Accidental | Revelación | B | 1 |
| Físico | Interno | Accidental | Modificación | B | 1 |
| Físico | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Físico | Interno | Accidental | Interrupción | B | 1 |
| Físico | Interno | Deliberado | Revelación | B | 3 |
| Físico | Interno | Deliberado | Modificación | B | 3 |
| Físico | Interno | Deliberado | Perdida/Destrucción | B | 3 |
| Físico | Interno | Deliberado | Interrupción | B | 3 |
| Físico | Externo | Accidental | Revelación | B | 1 |
| Físico | Externo | Accidental | Modificación | B | 1 |
| Físico | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Físico | Externo | Accidental | Interrupción | B | 1 |
| Físico | Externo | Deliberado | Revelación | B | 3 |
| Físico | Externo | Deliberado | Modificación | B | 3 |
| Físico | Externo | Deliberado | Perdida/Destrucción | B | 3 |
| Físico | Externo | Deliberado | Interrupción | B | 3 |

**Tabla 52. Probabilidad Servidores que contienen la plataforma para la publicación de las listas (físico)**

Para el activo **Sistema que realiza la calificación de las tarjetas de respuesta (maquina lectora):**

| Tipo | Actor | Motivo | Resultado | Probabili- | Punta- |
|---|---|---|---|---|---|

| de Acceso | | | | dad | je |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Deliberado | Revelación | B | 2 |
| Red | Interno | Deliberado | Modificación | B | 2 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 2 |
| Red | Interno | Deliberado | Interrupción | B | 2 |
| Red | Externo | Accidental | Revelación | B | 1 |
| Red | Externo | Accidental | Modificación | B | 1 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 1 |
| Red | Externo | Accidental | Interrupción | B | 1 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 53. Probabilidad Sistema que realiza la calificación de las tarjetas de respuesta (maquina lectora)**

Para el activo **Base de datos de personas inscritas:**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Delibera-do | Revelación | B | 1 |
| Red | Interno | Delibera-do | Modificación | B | 1 |
| Red | Interno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Interno | Delibera-do | Interrupción | B | 1 |
| Red | Ex-terno | Accidental | Revelación | B | 1 |
| Red | Ex-terno | Accidental | Modificación | B | 1 |
| Red | Ex-terno | Accidental | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Accidental | Interrupción | B | 1 |
| Red | Ex-terno | Delibera-do | Revelación | B | 1 |
| Red | Ex-terno | Delibera-do | Modificación | B | 1 |
| Red | Ex-terno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Delibera-do | Interrupción | B | 1 |

**Tabla 54. Probabilidad Base de datos de personas inscritas**

Para el activo **Plataforma de inscripciones:**

| **Tipo de Acce-so** | **Actor** | **Motivo** | **Resultado** | **Probabili-dad** | **Punta-je** |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdi-da/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Delibera-do | Revelación | B | 1 |
| Red | Interno | Delibera-do | Modificación | B | 1 |
| Red | Interno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Interno | Delibera-do | Interrupción | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Red | Ex-terno | Accidental | Revelación | B | 1 |
| Red | Ex-terno | Accidental | Modificación | B | 1 |
| Red | Ex-terno | Accidental | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Accidental | Interrupción | B | 1 |
| Red | Ex-terno | Delibera-do | Revelación | B | 1 |
| Red | Ex-terno | Delibera-do | Modificación | B | 1 |
| Red | Ex-terno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Delibera-do | Interrupción | B | 1 |

**Tabla 55. Probabilidad Plataforma de inscripciones**

Para el activo **Sistema integrado de recaudo (SQUID):**

| Tipo de Acce-so | Actor | Motivo | Resultado | Probabili-dad | Punta-je |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 1 |
| Red | Interno | Accidental | Modificación | B | 1 |
| Red | Interno | Accidental | Perdi-da/Destrucción | B | 1 |
| Red | Interno | Accidental | Interrupción | B | 1 |
| Red | Interno | Delibera-do | Revelación | B | 1 |
| Red | Interno | Delibera-do | Modificación | B | 1 |
| Red | Interno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Interno | Delibera-do | Interrupción | B | 1 |
| Red | Ex-terno | Accidental | Revelación | B | 1 |
| Red | Ex-terno | Accidental | Modificación | B | 1 |
| Red | Ex-terno | Accidental | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Accidental | Interrupción | B | 1 |
| Red | Ex- | Delibera- | Revelación | B | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | terno | do | | | |
| Red | Ex-terno | Delibera-do | Modificación | B | 1 |
| Red | Ex-terno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Delibera-do | Interrupción | B | 1 |

**Tabla 56. Probabilidad Sistema integrado de recaudo (SQUID)**

Para el activo **Personal de DARCA (Profesional especializado, el universitario):**

| **Tipo de Acce-so** | **Actor** | **Motivo** | **Resultado** | **Probabili-dad** | **Punta-je** |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 2 |
| Red | Interno | Accidental | Modificación | B | 2 |
| Red | Interno | Accidental | Perdi-da/Destrucción | B | 2 |
| Red | Interno | Accidental | Interrupción | B | 2 |
| Red | Interno | Delibera-do | Revelación | B | 3 |
| Red | Interno | Delibera-do | Modificación | B | 3 |
| Red | Interno | Delibera-do | Perdi-da/Destrucción | B | 3 |
| Red | Interno | Delibera-do | Interrupción | B | 3 |
| Red | Ex-terno | Accidental | Revelación | B | 2 |
| Red | Ex-terno | Accidental | Modificación | B | 2 |
| Red | Ex-terno | Accidental | Perdi-da/Destrucción | B | 2 |
| Red | Ex-terno | Accidental | Interrupción | B | 2 |
| Red | Ex-terno | Delibera-do | Revelación | B | 1 |
| Red | Ex-terno | Delibera-do | Modificación | B | 1 |
| Red | Ex-terno | Delibera-do | Perdi-da/Destrucción | B | 1 |
| Red | Ex-terno | Delibera-do | Interrupción | B | 1 |

**Tabla 57. Probabilidad Personal de DARCA (Profesional especializado, el universitario)**

Para el activo **Personal de TICS (ingeniero de soporte):**

| Tipo de Acceso | Actor | Motivo | Resultado | Probabilidad | Puntaje |
|---|---|---|---|---|---|
| Red | Interno | Accidental | Revelación | B | 2 |
| Red | Interno | Accidental | Modificación | B | 2 |
| Red | Interno | Accidental | Perdida/Destrucción | B | 2 |
| Red | Interno | Accidental | Interrupción | B | 2 |
| Red | Interno | Deliberado | Revelación | B | 3 |
| Red | Interno | Deliberado | Modificación | B | 3 |
| Red | Interno | Deliberado | Perdida/Destrucción | B | 3 |
| Red | Interno | Deliberado | Interrupción | B | 3 |
| Red | Externo | Accidental | Revelación | B | 2 |
| Red | Externo | Accidental | Modificación | B | 2 |
| Red | Externo | Accidental | Perdida/Destrucción | B | 2 |
| Red | Externo | Accidental | Interrupción | B | 2 |
| Red | Externo | Deliberado | Revelación | B | 1 |
| Red | Externo | Deliberado | Modificación | B | 1 |
| Red | Externo | Deliberado | Perdida/Destrucción | B | 1 |
| Red | Externo | Deliberado | Interrupción | B | 1 |

**Tabla 58. Probabilidad Personal de TICS (ingeniero de soporte)**

### 5.14 Matriz para valuación de activos y análisis de Riesgos.

La matriz de valuación de activos y análisis de riesgos se elaboro con el fin de mostrar los diferentes valores que se pueden obtener para cada amenaza y

probabilidad de impacto resultante de cada activo critico analizado. De esta forma se facilita tener todos los valores posibles del total de impacto del riesgo.

La explicación es la siguiente:

1. Existen 4 tipos de amenazas que son Revelación, Modificación, Perdida/Destrucción, Reputación. Por lo tanto, se elaboro una tabla para cada amenaza.
2. Cada amenaza afectaría cuatro variables que se comentaron en una primera instancia las cuales son reputación, seguridad/salud, productividad, financiero. Para cada variable se evaluó el impacto potencial de cada amenaza sobre dichas variables.
3. Se tomaron en cuenta los valores bajo, medio y alto (1, 2 y 3 respectivamente).
4. El valor mínimo para la suma de las variables para una amenaza es de 4, y el valor máximo es de 12. El resultado de la suma es el impacto de amenaza.
5. Cada valor de la suma para cada amenaza se multiplico por el factor de probabilidad de ocurrencia de dicha amenaza, la cual se midió de la misma forma, es decir bajo, medio y alto (1, 2 y 3 respectivamente).
6. El valor mínimo de la multiplicación de la suma de cada amenaza por el factor de probabilidad de ocurrencia de dicha amenaza es de 4, y el valor máximo es de 36.
7. Como existen amenazas que pueden ocurrir en situaciones deliberada y accidentalmente, tanto interna como externa a la organización, entonces se hizo la evaluación de cada tipo de amenaza para cada situación dicha. Por lo tanto se realizo la suma total de los valores resultantes en todas las situaciones, lo cual nos dio como resultado el valor total del riesgo para el activo critico.
8. El valor mínimo del valor total del riesgo es de 64, y el valor máximo es de 576.

A continuación se mostraran ilustraciones de las matrices de valuación de activos y análisis de riesgos.

Siler Amador Donado
D.N.I 72.168.640

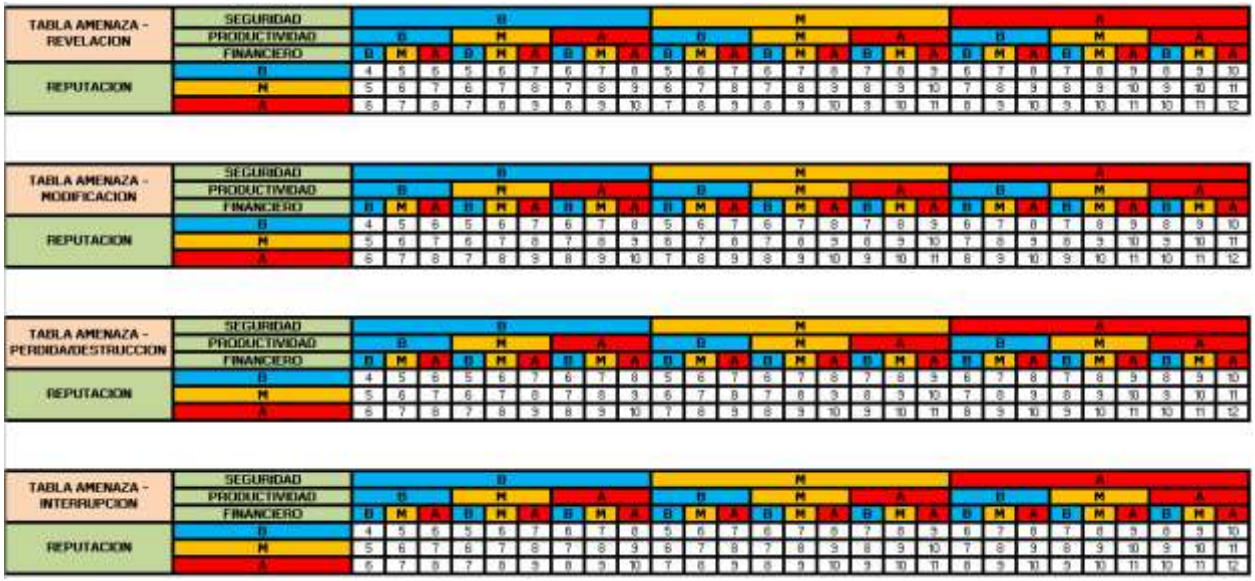


**Ilustración 9. Matriz de Impacto de Amenaza**

| VALORES TABLA AMENAZA | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 |
| 3 | 12 | 15 | 18 | 21 | 24 | 27 | 30 | 33 | 36 |

**Ilustración 10. Matriz de Impacto de Probabilidad**

| ACTOR | INTERNO | | | | | | | | EXTERNO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| MOTIVO | ACCIDENTAL | | | | DELIBERADO | | | | ACCIDENTAL | | | | DELIBERADO | | | | |
| AMENAZA | REVELACION | MODIFICACION | PERDIDA -DESTRUCCION | INTERRUPCION | REVELACION | MODIFICACION | PERDIDA -DESTRUCCION | INTERRUPCION | REVELACION | MODIFICACION | PERDIDA -DESTRUCCION | INTERRUPCION | REVELACION | MODIFICACION | PERDIDA - DESTRUCCION | INTERRUPCION | VALOR TOTAL IMPACTO DEL RIESGO |
| VALORES TOTALES DE IMPACTO DE RIESGO | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 64 |
| | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 80 |
| | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 96 |
| | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 112 |
| | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 128 |
| | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 144 |
| | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 160 |
| | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 11 | 176 |
| | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 192 |
| | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 14 | 224 |
| | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 15 | 240 |
| | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 256 |
| | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 288 |
| | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 320 |
| | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 336 |
| | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 22 | 352 |
| | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 24 | 384 |
| | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 27 | 432 |
| | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 480 |
| | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 33 | 528 |
| | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 36 | 576 |

**Ilustración 11. Matriz Valor del Riesgo**

El valor total del riesgo de los 15 activos críticos es el siguiente:

| Activo Critico | Valor del Riesgo | Procedimiento al cual pertenece el activo |
|---|---|---|
| Servidor que contiene la plataforma para la publicación de las listas | 194 | Evaluación de la prueba |
| Base de datos de personas inscritas | 168 | Inscripciones |
| Sistema integrado de recaudo(SQUID) | 64 | Admisiones |
| Plataforma de inscripciones | 152 | Inscripciones |
| Sistema que realiza la calificación de las tarjetas de respuesta(maquina lectora) | 110 | Evaluación de la prueba |
| Formularios | 48 | Aplicación de la prueba |
| Tarjetas de respuestas diligenciadas | 136 | Evaluación de la prueba |

| | | |
|---|---|---|
| Material empacado y sellado en bolsas de seguridad | 146 | Evaluación de la prueba, Aplicación de la prueba |
| Claves de respuesta (respuestas correctas) | 64 | Evaluación de la prueba |
| Archivo cifrado del documento que almacena los puntajes de los aspirantes en orden descendentes cargado en SIMCA | 139 | Evaluación de la prueba |
| Convenio de cooperación interadministrativo suscrito entre la universidad de Antioquia y la Universidad del Cauca | 88 | Alistamiento para la aplicación de la prueba |
| Archivos de inscripción | 159 | Inscripciones |
| Credenciales de citación | 164 | Alistamiento para la aplicación de la prueba |
| Personal de DARCA (Profesional especializado, el universitario) | 83 | Evaluación de la prueba |
| Personal de TICS (ingeniero de soporte) | 83 | Evaluación de la prueba |

**Tabla 59. Valor total del riesgo por activos**

El valor total del riesgo por cada procedimiento es el siguiente:

| Procedimiento | Valor del Riesgo |
|---|---|
| Evaluación de la Prueba | 955 |
| Inscripciones | 645 |
| Aplicación de la Prueba | 460 |
| Alistamiento para la Aplicación de la Prueba | 418 |
| Admisiones | 230 |

**Tabla 60. Valor total del riesgo por procedimientos**

Con el fin de lograr resultados a corto plazo, se toma la decisión de escoger un solo procedimiento (el más crítico), al cual se le realiza la gestión del riesgo.

Al analizar la anterior tabla, se puede notar que el procedimiento con valor del riesgo más alto (el más crítico) es el procedimiento *Evaluación de la Prueba*. Por lo tanto la gestión del riesgo se analizó a dicho procedimiento.

### 5.15 Estrategia de Protección del procedimiento Evaluación de la Prueba (paso 25)

En el paso 25, se determinó la estrategia de protección actual en DARCA para cada una de las 15 áreas de práctica de seguridad con respecto al procedimiento Evaluación de la Prueba. Esto con el fin de observar que tan bien están iniciando, implementando y manteniendo su seguridad interna, así como que actividades se están ejecutando como estrategia de protección, en donde se puede determinar qué actividad podría estar faltando y que al faltar, podría ocasionar un riesgo tanto para los activos críticos como para el proceso Inscripciones y Admisiones con respecto al procedimiento Evaluación de la Prueba.

Para el **área 1. Conciencia y Formación de Seguridad**:

- La organización cuenta con una estrategia de formación informal y no documentado.
- En cuanto a capacitación en temas de seguridad, se orientan unos lineamientos básicos mas no especializados.
- No hay un plan de capacitación en seguridad para las Tecnologías Soportadas.
- La organización no tiene un mecanismo para proporcionar a los miembros del personal actualizaciones periódicas / boletines sobre los problemas de seguridad importantes.
- La organización cuenta con mecanismos informales para el seguimiento y la verificación de que los funcionarios reciben capacitación en materia de seguridad apropiada.

Para el **área 2. Estrategia de Seguridad:**

- La organización cuenta con mecanismos informales para la integración de:
  - Consideraciones de seguridad en las estrategias de negocio
  - Estrategias y metas en las estrategias y políticas de seguridad empresariales.
- La organización cuenta con estrategias informales e indocumentadas de seguridad, metas y objetivos.
- El programa de formación de la conciencia de seguridad de la organización no incluye información sobre la estrategia de seguridad de la organización. Los miembros del personal aprenden sobre la estrategia de seguridad de la organización por su cuenta.

Para el **área 3. Gestión de la Seguridad:**

- La organización cuenta con los roles y responsabilidades de seguridad de información informales e indocumentados.
- El presupuesto de la organización cuenta con una partida distinta de las actividades de seguridad de la información. El nivel de financiamiento se determina mediante procesos informales.

- La organización dispone de procedimientos informales e indocumentados para la inclusión de las consideraciones de seguridad en los procesos de contratación (por ejemplo, verificación de antecedentes) y terminación (por ejemplo, eliminar el acceso a todos los sistemas y la información) de la organización.
- La organización cuenta con un proceso definido formalmente para evaluar sus riesgos de seguridad de la información. El proceso de gestión de riesgos de seguridad de la información es informal y no documentado.
- No existe un programa de capacitación formal en conciencia de personal, pero la formación se realiza sobre las situaciones o consideraciones que se presenten.
- La organización no tiene un mecanismo para proporcionar a los gerentes los resúmenes de la información relacionada con la seguridad importante.

Para el **área 4. Políticas y Reglamentos de Seguridad:**

- Las políticas relacionadas con la seguridad de la organización son informales e indocumentados.
- La organización cuenta con un mecanismo informal y no documentado para crear y actualizar sus políticas relacionadas con la seguridad.
- La organización dispone de procedimientos informales e indocumentados para hacer cumplir sus políticas relacionadas con la seguridad.
- El programa de capacitación en conciencia de la seguridad de la organización no incluye información sobre las políticas y las normas de seguridad de la organización. Los miembros del personal aprenden sobre las políticas y las normas de seguridad por su cuenta.
- La organización dispone de procedimientos informales e indocumentados para el cumplimiento de las políticas de información de seguridad, las leyes y reglamentos aplicables, y los requisitos de seguro.

Para el **área 5. Gestión de la Seguridad Colaborativa:**

- La organización ha documentado políticas y procedimientos para proteger la información a la hora de trabajar con los colaboradores y socios (En admisiones si, en SIMCA no).
- La organización cuenta con políticas y procedimientos informales e indocumentados para proteger la información cuando se trabaja con los contratistas y subcontratistas.
- La organización cuenta con políticas y procedimientos informales e indocumentados para proteger la información cuando se trabaja con los proveedores de servicios.
- La organización comunica de manera informal los requisitos de protección de información a todas las terceras partes apropiadas.
- La organización no tiene los mecanismos para verificar que todas las organizaciones de terceros, servicios de seguridad externalizados, mecanismos y tecnologías cumplen sus necesidades y requerimientos.
- No tienen programa de conciencia de personal

Para el **área 6. Planes de Contingencia / Recuperación de Desastres:**

- No se ha realizado un análisis de las operaciones, las aplicaciones y la criticidad de los datos.

- La organización no ha documentado la continuidad del negocio o de los planes de operaciones de emergencia, el plan (s) de recuperación de desastres, y el plan (s) de contingencia para responder a las emergencias. Algunos aspectos de los planes son informales e indocumentados.
- El acceso físico y electrónico a la información crítica no se tiene en cuenta formalmente en contingencia, recuperación de desastres y planes de continuidad de negocio de la organización.
- No hay plan en conciencia de personal.

Para el **área 7. Control de Acceso Físico:**

- La organización cuenta con planes y procedimientos informales e indocumentados para el control de acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software.
- No hay planes de capacitación que incluya una revisión de los planes y procedimientos para el control de acceso físico de la organización.
- Los requisitos de la organización para el control de acceso físico están informalmente comunicados a todos los contratistas y proveedores de servicios que controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para el control de acceso físico.

Para el **área 8. Monitoreo y Auditoría de Seguridad Física:**

- DARCA cuenta con algunas de las políticas y procedimientos formalmente documentados para supervisar el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software. Algunas políticas y procedimientos en esta área son informales e indocumentados.
- Los miembros del personal designados pueden asistir a la capacitación para el monitoreo de acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, software y medios de comunicación si la solicitan.
- Los requisitos de DARCA para el seguimiento de la seguridad física se comunicarán formalmente a todos los contratistas y proveedores de servicios que controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software.
- DARCA verifica formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el monitoreo de la seguridad física.
- Los requisitos de DARCA para el seguimiento de la seguridad física son informalmente comunicados a todos los contratistas y proveedores de servicios que controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software.
- DARCA verifica formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el monitoreo de la seguridad física.

Para el **área 9. Gestión de Sistema y Red:**

- La organización cuenta con algunos procedimientos del sistema de gestión de red y formalmente documentadas. Algunos procedimientos de esta área son informales e indocumentados.

- Los miembros del personal de tecnología de la información pueden asistir a la capacitación para la gestión de sistemas y redes y el uso de sistemas y herramientas de gestión de red en caso de que lo soliciten.
- Los requerimientos de gestión de redes y sistemas relacionados con la seguridad de la organización son informalmente comunicados a todos los contratistas y proveedores de servicios que mantienen sistemas y redes.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para el sistema relacionado con la seguridad y gestión de red.

Para el **área 10. Seguimiento y auditoría de TI Seguridad:**

- La organización dispone de procedimientos informales e indocumentados para el monitoreo de acceso de sistemas y redes basada en la red.
- Los miembros del personal de tecnología de la información pueden asistir a la capacitación para el monitoreo de acceso basada en la red de sistemas y redes y el uso de herramientas de monitoreo y auditoría si la solicitan.
- Los requisitos de la organización para el seguimiento de la información de seguridad de tecnología se comunican de manera informal a todos los contratistas y proveedores de servicios que controlan los sistemas y redes.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la vigilancia de la seguridad informática.

Para el **área 11. Autenticación y autorización:**

- La organización cuenta con algunos de los procedimientos de autorización y autenticación formalmente documentados para restringir el acceso de los usuarios a la información, los sistemas sensibles, aplicaciones y servicios específicos, y las conexiones de red. Algunos procedimientos de esta área son informales e indocumentados.
- Los miembros del personal de tecnología de la información pueden asistir a la capacitación para la aplicación de medidas tecnológicas para restringir el acceso de los usuarios a la información, los sistemas sensibles, aplicaciones y servicios específicos, y las conexiones de red en caso de que lo soliciten.
- Los requisitos de la organización para el control de acceso a los sistemas y la información están informalmente comunicados a todos los contratistas y proveedores de servicios que controlan los sistemas y redes.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la autenticación y autorización.

Para el **área 12. Gestión de Vulnerabilidades:**

- La organización cuenta con algunos de los procedimientos de gestión de vulnerabilidades formalmente documentados. Algunos procedimientos de esta área son informales e indocumentados.
- Los miembros del personal de tecnología de la información pueden asistir a la capacitación para la gestión de vulnerabilidades tecnológicas y el uso de herramientas de evaluación de la vulnerabilidad en caso de que lo soliciten.

- Los requisitos de gestión de la vulnerabilidad de la organización son informalmente comunicados a todos los contratistas y proveedores de servicios que gestionan las vulnerabilidades tecnológicas.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la gestión de vulnerabilidades.

Para el **área 13. Cifrado:**

- La organización cuenta con algunos procedimientos formalmente documentados para la implementación y uso de tecnologías de cifrado. Algunos procedimientos de esta área son informales e indocumentados.
- Los miembros del personal de tecnología de la información pueden asistir a la capacitación para la implementación de tecnologías de cifrado si lo solicitan.
- Todos los miembros del personal pueden asistir a la capacitación para el uso de tecnologías de cifrado si lo solicitan.
- Los requisitos de la organización para la protección de la información sensible se comunican de manera informal a todos los contratistas y proveedores de servicios que proporcionan las tecnologías de cifrado.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la aplicación de tecnologías de cifrado.

Para el **área 14. Arquitectura y Diseño de Seguridad:**

- La organización cuenta con prácticas de arquitectura y diseño de seguridad formalmente documentada. Algunas prácticas en este ámbito son informales e indocumentados.
- Los miembros del personal pueden asistir a la capacitación para el diseño de los sistemas y las redes seguras, si lo solicitan.
- Los requisitos relacionados con la seguridad de la organización son informalmente comunicados a todos los contratistas y proveedores de servicios que diseñan sistemas y redes.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la arquitectura y el diseño de la seguridad.

Para el **área 15. Gestión de Incidentes:**

- La organización cuenta con unos procedimientos de gestión de incidentes documentados formalmente. Algunos procedimientos de esta área son informales e indocumentados.
- Los miembros del personal designados pueden asistir a la capacitación para la gestión de incidencias, si así lo solicitan.
- Los requisitos de la organización para la gestión de incidentes se comunican de manera informal a todos los contratistas y proveedores de servicios que ofrecen servicios de gestión de incidentes.
- La organización verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la gestión de incidencias.

### 5.16 Perfil de riesgo de Información - Selección de áreas de mitigación (Pasos 26 y 27)

En el paso 26 se transfirió el estado de luz para cada área de práctica de seguridad descrita en los pasos 3 y 4 (verde, amarillo, rojo). Luego se seleccionaron las áreas de mitigación; su escogencia se basó en lo siguiente:

- Perfil de riesgo (para cada activo crítico)
- Activos Críticos (para cada activo crítico)
- Prácticas de Seguridad
- Revisión de Infraestructura
- Criterios de Evaluación de Impacto
- Criterios de Evaluación Probabilidad
- Los riesgos para los activos críticos

En el paso 27 se definió el enfoque para abordar cada riesgo a los activos críticos con respecto a las áreas a mitigar en el paso 26. Para ello se tomó como referencia tres tomas de decisiones diferentes:

- **Aceptar**: es una decisión tomada durante el análisis de riesgo donde no se llevará a cabo alguna medida para hacer frente a un riesgo y donde se acepta las consecuencias si el riesgo ocurre. Los riesgos que se aceptan generalmente tienen un bajo impacto en una organización.
- **Mitigar**: es una decisión tomada durante el análisis de riesgo donde se llevará a cabo medidas para hacer frente a un riesgo mediante la implementación de actividades diseñadas para contrarrestar la amenaza. Los riesgos que se mitigan suelen tener un alto impacto en una organización.
- **Aplazar**: es una decisión en la que el riesgo no ha sido aceptado ni mitigado. El impacto en la organización, debido al riesgo diferido está por encima de un umbral mínimo, pero no tan grande como para ser una prioridad inmediata. Los riesgos diferidos son observados y evaluados nuevamente en algún momento en el futuro.

La decisión fue tomada por el directo de DARCA, el cual fue “Mitigar”.

### 5.17 Plan de Mitigación del procedimiento Evaluación de la Prueba (paso 28)

En este paso se desarrolló un plan de mitigación para cada área de práctica de seguridad en estado rojo y amarillo. Para hacer esto se retomó la información de:

- Prácticas de Seguridad
- Estrategia de Protección
- Perfil de riesgo (para cada activo crítico)
- Información de Activos Críticos (para cada activo crítico)

Estos planes de mitigación de riesgos se diseñaron para reducir los riesgos que podrían impedir que el proceso Inscripciones y Admisiones en DARCA, con respecto al procedimiento Evaluación de la Prueba logren su misión. Las actividades de mitigación diseñadas abordan las amenazas en una o más de las siguientes formas:

- Reconocer las amenazas a medida que ocurran.
- Resistir las amenazas para evitar que se produzcan.
- Recuperarse de las amenazas después de que ocurran.

Los planes de mitigación de riesgos diseñados comprenden los siguientes elementos:

- La actividad de mitigación: En esta parte se definieron las actividades diseñadas para implementar en un área de práctica de seguridad.
- La razón fundamental: En esta parte se documento las razones para la selección de cada actividad de mitigación; se documento si la actividad tiene la intención de reconocer las amenazas, resistirse a ellos, o para recuperarse de ellos.
- Responsabilidad de mitigación: En esta parte se identificó quien o quienes deben estar asociados en la ejecución de cada actividad.
- Apoyo adicional: En esta parte se documentó cualquier apoyo adicional necesario para la aplicación de cada actividad (por ejemplo, la financiación, el compromiso del personal, patrocinio).

Los resultados para cada área (con color de estado amarillo y rojo) son las siguientes:

Para el **área 1. Conciencia y Formación de Seguridad**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Elaborar una estrategia de capacitación documentada que incluya concienciación sobre la seguridad y la formación relacionada con la seguridad para las | Las políticas relacionadas con la seguridad del procedimiento Evaluación de la Prueba son informales e indocumentadas. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| tecnologías compatibles en el procedimiento de Evaluación de la Prueba. | | |
| Proporcionar dos veces al año lecciones de concienciación especializada, sobre la seguridad de la información, del procedimiento Evaluación de la Prueba. | Los lineamientos de formación que se imparten son básicos y no especializados. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Elaborar un plan de capacitación en seguridad para las tecnologías soportadas en el procedimiento Evaluación de la Prueba. | Las tecnologías que se usan en el procedimiento de evaluación de la prueba se actualizan regularmente, por lo tanto se necesita que el personal responsable de su manejo conozca los requisitos de seguridad para dichas tecnologías. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar un mecanismo formal para proporcionar a los miembros del personal con actualizaciones periódicas / boletines sobre los problemas de seguridad importantes sobre el | No tiene mecanismo. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| procedimiento Evaluación de la Prueba. | | |
| Diseñar mecanismos formales para el seguimiento y la verificación de que los funcionarios encargados del procedimiento Evaluación de la Prueba reciben capacitación en materia de seguridad apropiada. | Tienen mecanismos informales. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

**Tabla 61. Controles Conciencia y Formación de Seguridad**

Para el **área 2. Estrategia de Seguridad**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar las estrategias de seguridad, metas y objetivos del procedimiento Evaluación de la Prueba de manera formal. | DARCA cuenta con estrategias informales e indocumentados de seguridad, metas y objetivos | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Elaborar un programa de formación de la conciencia de seguridad donde se incluya información sobre la estrategia de seguridad del procedimiento Evaluación de la Prueba. | El programa de formación de la conciencia de seguridad de DARCA no incluye información sobre la estrategia de seguridad de DARCA. Los miembros del personal a aprender sobre la | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| También proporcionar esta formación para todos los empleados dos veces al año. | estrategia de seguridad de DARCA por su cuenta. | |

**Tabla 62. Controles Estrategia de Seguridad**

Para el **área 4. Políticas y Reglamentos de Seguridad**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente las políticas relacionadas con la seguridad del procedimiento Evaluación de la Prueba. | Las políticas relacionadas con la seguridad de DARCA son informales e indocumentadas. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Crear un mecanismo formal y documentado para la creación y actualización de las políticas relacionadas con la seguridad del procedimiento Evaluación de la Prueba. | DARCA cuenta con un mecanismo informal y no documentado para crear y actualizar sus políticas relacionadas con la seguridad. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Documentar procedimientos formales para hacer cumplir las políticas relacionadas con la seguridad del procedimiento Evaluación de la Prueba. Los procedi- | DARCA dispone de procedimientos informales e indocumentados para hacer cumplir sus políticas relacionadas con la seguridad. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| mientos de ejecución se deben seguir consistentemente. | | |
| Incluir información sobre las políticas y las normas de seguridad del procedimiento Evaluación de la Prueba en el programa de capacitación en seguridad de la conciencia. Proporcionar esta formación para todos los empleados dos veces al año. | El programa de capacitación en conciencia de la seguridad de DARCA no incluye información sobre las políticas y las normas de seguridad de DARCA. Los miembros del personal aprenden sobre las políticas y las normas de seguridad por su cuenta. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Documentar procedimientos formales para el cumplimiento de las políticas de información de seguridad, las leyes y reglamentos aplicables, y los requisitos de seguro con respecto al procedimiento Evaluación de la Prueba. | DARCA dispone de procedimientos informales e indocumentados para el cumplimiento de las políticas de información de seguridad, las leyes y reglamentos aplicables, y los requisitos de seguro. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar políticas, procedimientos y controles formales de intercambio con objeto de proteger la información del proce- | No existen políticas, procedimientos y controles formales de intercambio con objeto de proteger la informa- | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| dimiento Evaluación de la Prueba mediante el uso de todo tipo de servicios de comunicación. | ción del procedimiento de Evaluación de la prueba mediante el uso de todo tipo de servicios de comunicación. | |
| Diseñar políticas para escritorios y monitores limpios de información del procedimiento Evaluación de la Prueba. | No existen políticas para escritorios y monitores limpios de información referente al procedimiento Evaluación de la prueba | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

**Tabla 63. Controles Políticas y Reglamentos de Seguridad**

Para el **área 5. Gestión de la Seguridad Colaborativa**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar políticas y procedimientos formalmente para proteger la información del procedimiento de Evaluación de la Prueba cuando se trabaja con los contratistas y subcontratistas. | DARCA cuenta con políticas y procedimientos para proteger la información cuando se trabaja con los contratistas y subcontratistas, pero dichas políticas son informales e indocumentadas. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Documentar políticas y procedimientos para proteger la información del procedimiento Evaluación de la Prueba | DARCA cuenta con políticas y procedimientos para proteger la información cuando se trabaja con los proveedo- | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| cuando se trabaja con los proveedores de servicios. | res de servicios informales e indocumentados. | |
| Documentar procedimientos formales para hacer cumplir las políticas relacionadas con la seguridad del procedimiento Evaluación de la Prueba. Los procedimientos de ejecución se deben seguir consistentemente. | DARCA comunica de manera informal los requisitos de protección de información a todas las terceras partes apropiadas. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar mecanismos formales para verificar que todas las organizaciones de terceros, servicios de seguridad externalizados, mecanismos y tecnologías cumplen sus necesidades y requerimientos con respecto al procedimiento Evaluación de la Prueba. | DARCA no tiene los mecanismos para verificar que todas las organizaciones de terceros, servicios de seguridad externalizados, mecanismos y tecnologías cumplen sus necesidades y requerimientos. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar un programa de capacitación en seguridad de la conciencia donde se incluya información sobre las | No tiene programa | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| políticas de gestión de la seguridad colaborativa del procedimiento Evaluación de la Prueba. Proporcionar esta formación para todos los empleados dos veces al año. | | |

**Tabla 64. Controles Gestión de la Seguridad Colaborativa**

Para el **área 6. Planes de Contingencia / Recuperación de Desastres**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Realizar un análisis total de las operaciones, las aplicaciones y la criticidad de los datos del procedimiento Evaluación de la Prueba. | No se ha realizado un análisis de las operaciones, las aplicaciones y la criticidad de los datos del procedimiento Evaluación de la prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Documentar formalmente y poner a prueba la continuidad del negocio o de los planes de operaciones de emergencia, el plan (s) de recuperación de desastres, y el plan (s) de contingencia para responder a las emergencias que puedan poner en riesgo el procedimiento Evaluación de | No hay plan. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| la Prueba. | | |
| Considerar como factor en contingencia, recuperación de desastres y planes de continuidad de negocio de DARCA, el acceso físico y electrónico a la información crítica del procedimiento Evaluación de la Prueba. | El acceso físico y electrónico a la información crítica del procedimiento Evaluación de la Prueba no se factoriza formalmente en contingencia, recuperación de desastres y planes de continuidad de negocio de DARCA. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar un programa de capacitación en conciencia de la seguridad donde incluya información sobre la contingencia de DARCA, recuperación de desastres y planes de continuidad del negocio con respecto al procedimiento Evaluación de la Prueba. También proporcionar esta formación para todos los empleados dos veces al año. | No tienen plan | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Identificar los eventos que puedan causar interrupciones a los | No se identifican los eventos que puedan causar interrupciones a | Profesional Especializado porque es el encargado de todo el procedimiento |

| | | |
|---|---|---|
| procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información del procedimiento Evaluación de la Prueba. | los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información del procedimiento Evaluación de la Prueba. | Evaluación de la Prueba. |

**Tabla 65. Controles Planes de Contingencia / Recuperación de Desastres**

Para el **área 7. Control de Acceso Físico**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente los planes y procedimientos de control de acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software que tengan que ver con el procedimiento Evaluación de la Prueba. | DARCA cuenta con planes y procedimientos informales e indocumentados para el control de acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software que tenga que ver con el procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar un plan que incluya una revisión de los planes y procedimientos para el control de acceso físico que contenga el procedi- | No hay plan que incluya una revisión de los planes y procedimientos para el control de acceso físico, para que los miembros del personal | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| miento Evaluación de la Prueba, y se debe requerir que los miembros del personal designados asistan a dicha capacitación. | designados puedan asistir a dicha capacitación si lo solicitan en DARCA. | |
| Informar formalmente los requisitos para el control de acceso físico, a todos los contratistas y proveedores de servicios que controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software en donde intervenga el procedimiento Evaluación de la Prueba. | Los requisitos de DARCA para el control de acceso físico que maneje el procedimiento Evaluación de la Prueba están informalmente comunicados a todos los contratistas y proveedores de servicios que controlan el acceso físico al edificio y las instalaciones, áreas de trabajo, hardware, y soporte de software. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Verificar formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para el control de acceso físico con respecto al procedimiento Evaluación de la Prueba. | DARCA verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para el control de acceso físico que tenga que ver con el procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| Permitir que los sistemas sensibles que intervienen en el procedimiento Evaluación de la Prueba, dispongan de un entorno informático dedicado (propio). | Los sistemas sensibles no disponen de un entorno informático dedicado (propio). | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

**Tabla 66. Controles Control de Acceso Físico**

Para el **área 10. Seguimiento y auditoría de TI Seguridad**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente los procedimientos de seguimiento de acceso de sistemas y redes basadas en la red q involucre el procedimiento Evaluación de la Prueba. | DARCA dispone de procedimientos informales e indocumentados para el monitoreo de acceso de sistemas y redes basada en la red q involucre el procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Solicitar a los miembros del personal de tecnología de información involucrados en el procedimiento Evaluación de la Prueba que asistan a la capacitación para el monitoreo de acceso basada en la red de sistemas y redes y el | Los miembros del personal de tecnología de la información involucrados en el procedimiento Evaluación de la Prueba pueden asistir a la capacitación para el monitoreo de acceso basada en la red de sistemas y redes y el uso | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| uso de herramientas de monitoreo y auditoría. | de herramientas de monitoreo y auditoría si la solicitan. | |
| Comunicar formalmente a todos los contratistas y proveedores de servicios que controlan los sistemas y redes que involucra el procedimiento Evaluación de la Prueba, los requisitos de DARCA para el seguimiento de la información de seguridad de tecnología para el procedimiento detallado anteriormente. | Los requisitos de DARCA para el seguimiento de la información de seguridad de tecnología se comunican de manera informal a todos los contratistas y proveedores de servicios que controlan los sistemas y redes. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Verificar formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el monitoreo de la seguridad informática del procedimiento Evaluación de la Prueba. | DARCA verifica de manera informal que los contratistas y los proveedores de servicios se han cumplido los requisitos para la vigilancia de la seguridad informática que involucre el procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

**Tabla 67. Controles Seguimiento y auditoría de TI Seguridad**

Para el **área 12. Gestión de Vulnerabilidades**:

Siler Amador Donado
D.N.I 72.168.640

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente todos los procedimientos de gestión de vulnerabilidades que involucre el procedimiento Evaluación de la Prueba. | DARCA cuenta con algunos de los procedimientos de gestión de vulnerabilidades formalmente documentados. El problema es que algunos procedimientos de esta área que involucran el procedimiento Evaluación de la Prueba son informales e indocumentados. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Solicitar que los miembros del personal de tecnología de información involucrados en el procedimiento Evaluación de la Prueba que asistan a la capacitación para la gestión de vulnerabilidades tecnológicas y el uso de herramientas de evaluación de la vulnerabilidad. No se debe esperar que ellos lo soliciten. | Los miembros del personal de tecnología de la información involucrados en el procedimiento Evaluación de la Prueba pueden asistir a la capacitación para la gestión de vulnerabilidades tecnológicas y el uso de herramientas de evaluación de la vulnerabilidad en caso de que lo soliciten. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Comunicar formalmente | Los requisitos de gestión | Profesional Especializado |

| | | |
|---|---|---|
| los requisitos de gestión de la vulnerabilidad del procedimiento Evaluación de la Prueba, a todos los contratistas y proveedores de servicios que gestionan las vulnerabilidades tecnológicas de la misma. | de la vulnerabilidad de DARCA están informalmente comunicados a todos los contratistas y proveedores de servicios que gestionan las vulnerabilidades tecnológicas para el procedimiento Evaluación de la Prueba. | porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Verificar formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la gestión de vulnerabilidades del procedimiento Evaluación de la Prueba. | DARCA verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la gestión de vulnerabilidades para el procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

**Tabla 68. Controles Gestión de Vulnerabilidades**

Para el **área 13. Cifrado**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente todos los procedimientos para la implementación y el uso de tecnologías de cifrado que intervengan en el procedimiento Evalua- | DARCA cuenta con algunos procedimientos formalmente documentados para la implementación y uso de tecnologías de cifrado que intervienen en el procedimiento Evalua- | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| ción de la Prueba. | ción de la Prueba. El problema es que algunos procedimientos de esta área son informales e indocumentados. | |
| Solicitar que los miembros del personal de tecnología de información involucrados en el procedimiento Evaluación de la Prueba asistan a la capacitación para el uso e implementación de tecnologías de cifrado. | Los miembros del personal de tecnología de la información involucrados en el procedimiento Evaluación de la Prueba pueden asistir a la capacitación para el uso e implementación de tecnologías de cifrado si lo solicitan. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Comunicar formalmente los requisitos de DARCA para la protección de la información sensible del procedimiento Evaluación de la Prueba, a todos los contratistas y proveedores de servicios que proporcionan las tecnologías de cifrado. | Los requisitos de DARCA para la protección de la información sensible del procedimiento Evaluación de la Prueba se comunican de manera informal a todos los contratistas y proveedores de servicios que proporcionan las tecnologías de cifrado. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Verificar formalmente que los contratistas y los proveedores de servicios | DARCA verifica de manera informal que los contratistas y los provee- | Profesional Especializado porque es el encargado de todo el procedimiento |

| | | |
|---|---|---|
| que intervienen en el procedimiento Evaluación de la Prueba han cumplido los requisitos para la aplicación de tecnologías de cifrado. | dores de servicios involucrados en el procedimiento Evaluación de la Prueba han cumplido los requisitos para la aplicación de tecnologías de cifrado. | Evaluación de la Prueba. |

**Tabla 69. Controles Cifrado**

Para el **área 14. Arquitectura y Diseño de Seguridad**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente todas las prácticas de arquitectura y de diseño de seguridad para el procedimiento Evaluación de la Prueba. | DARCA cuenta con prácticas de arquitectura y diseño de seguridad para el procedimiento Evaluación de la Prueba formalmente documentada. El problema es que algunas prácticas en este ámbito son informales e indocumentadas. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Solicitar que los miembros del personal involucrados en el procedimiento Evaluación de la Prueba, asistan a la capacitación para el diseño de sistemas y redes seguras. | Los miembros del personal involucrados en el procedimiento Evaluación de la Prueba pueden asistir a la capacitación para el diseño de los sistemas y las redes seguras, si lo solicitan. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| Comunicar formalmente a todos los contratistas y proveedores de servicios que diseñan sistemas y redes, los requisitos relacionados con la seguridad del procedimiento Evaluación de la Prueba. | Los requisitos relacionados con la seguridad de DARCA y el procedimiento Evaluación de la Prueba están informalmente comunicados a todos los contratistas y proveedores de servicios que diseñan sistemas y redes. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Verificar formalmente que los contratistas y los proveedores de servicios han cumplido los requisitos para la arquitectura y el diseño de la seguridad del procedimiento Evaluación de la Prueba. | DARCA verifica de manera informal que los contratistas y los proveedores de servicios han cumplido los requisitos para la arquitectura y el diseño de la seguridad correspondiente al procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

**Tabla 70. Controles Arquitectura y Diseño de Seguridad**

Para el **área 15. Gestión de Incidentes**:

| **Actividad de Mitigación** | **Razón Fundamental** | **Responsabilidad de Mitigación** |
|---|---|---|
| Documentar formalmente todos los procedimientos de gestión de incidentes para el procedimiento | DARCA cuenta con unos procedimientos de gestión de incidentes para el procedimiento Evaluación de la prueba documentados formal- | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| Evaluación de la Prueba. | mente. El problema es que algunos procedimientos de esta área son informales e indocumentados. | |
| Solicitar que los funcionarios designados para el procedimiento Evaluación de la Prueba asistan a la capacitación para la gestión de incidencias. No esperar a que dichos funcionarios la soliciten. | Los miembros del personal designados para el procedimiento Evaluación de la Prueba pueden asistir a la capacitación para la gestión de incidencias, si así lo solicitan. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Comunicar formalmente a todos los contratistas y proveedores de servicios que ofrecen servicios de gestión de incidentes, los requisitos de DARCA para la gestión de incidentes del procedimiento Evaluación de la Prueba. | Los requisitos de DARCA para la gestión de incidentes se comunican de manera informal a todos los contratistas y proveedores de servicios que ofrecen servicios de gestión de incidentes para el procedimiento Evaluación de la Prueba. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Verificar formalmente que los contratistas y los proveedores de servicios involucrados en el procedimiento Evalua- | DARCA verifica de manera informal que los contratistas y los proveedores de servicios involucrados en el pro- | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |

| | | |
|---|---|---|
| ción de la Prueba han cumplido los requisitos para la gestión de incidencias. | cedimiento Evaluación de la Prueba han cumplido los requisitos para la gestión de incidencias. | |
| Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información involucrados en el procedimiento Evaluación de la Prueba deben anotar y comunicar cualquier debilidad observada o sospechada en la seguridad del mismo. | Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información involucrados en el procedimiento Evaluación de la Prueba, no anotan y comunican cualquier debilidad observada o sospechada en la seguridad de los mismos. | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba. |
| Diseñar un mecanismo que permita cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información del procedimiento Evaluación de la Prueba. | No existe un mecanismo que permita cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información del procedimiento Evaluación de la Prueba | Profesional Especializado porque es el encargado de todo el procedimiento Evaluación de la Prueba |

**Tabla 71. Controles Gestión de Incidentes**

### 5.18 Resultado de los Controles y Porcentaje de Reducción del Riesgo (paso 29)

Para el tratamiento de las áreas a mitigar, solo se propuso controles para las áreas amarillas y rojas, pero solo se implementaron dos controles (un control por

área), los cuales se implementaron para el área 2 y el área 6. El resto de tratamiento queda para trabajos futuros, en donde se decide si es factible o no imimplementar los controles restantes para el tratamiento del riesgo en base al costo del control y lo que esto beneficiaria al procedimiento Evaluación de la Prueba y al proceso Inscripciones y Admisiones.

Los controles implementados fueron los siguientes:

En el **Área 2. Estrategia de seguridad**:

Se documentaron las estrategias de seguridad, metas y objetivos del procedimiento Evaluación de la Prueba de manera formal. Fue realizado por el Profesional Especializado debido a que es el encargado de todo el procedimiento Evaluación de la Prueba.

En el **Área 6. Planes de Contingencia / Recuperación de Desastres**:

Se identificaron los eventos que pudieran causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información del procedimiento Evaluación de la Prueba. Fue realizado por el Profesional Especializado debido a que es el encargado de todo el procedimiento Evaluación de la Prueba.

Luego de haber implementado los controles, se volvió a medir el riesgo al proceso Inscripciones y Admisiones.

A cada activo se le identifico sus amenazas, el impacto de dichas amenazas y la probabilidad de ocurrencia de dichas amenazas. Para definir la probabilidad, se basó en las 15 áreas sugeridas en OCTAVE-S, identificando qué activos están asociados a dichas áreas; a las áreas que tenían implementada menos controles o ninguno, tenían una probabilidad más alta de ocurrencia de un incidente de seguridad. Luego de aplicar controles en las áreas mencionadas, la probabilidad se redujo beneficiando a los activos asociado a cada unas de las áreas en las que se implantaron los controles. Al ser la probabilidad (1=bajo, 2= medio, 3= alto) un factor multiplicador del valor del impacto, nos permite visualizar cuantitativamente como va reduciendo el valor del riesgo para cada activo involucrado en todos los procedimientos del proceso inscripciones y admisiones.

Los resultados son los siguientes para cada activo:

| Activo | Valor Total Impacto del Riesgo sin los controles implanta-dos | Valor Total Impacto del Riesgo con los controles implanta-dos |
|---|---|---|
| Archivo cifrado del docu-mento que almacena los puntajes | 139 | 139 |
| Claves de respues-ta(Respuestas Correctas) | 64 | 64 |
| Material Empacado y Sellado en bolsas de Seguridad | 204 | 170 |
| Tarjetas de respuesta diligenciadas | 136 | 136 |
| Servidores que contienen la plataforma para la publicación de las listas | 279 | 279 |
| Sistema que realiza la calificación de las tarjetas de respuesta(maquina lectora) | 134 | 134 |
| Personal DARCA | 134 | 90 |
| Personal TICS | 134 | 90 |
| Archivos de Inscripción | 159 | 159 |
| Convenio de cooperación interadministrativo | 88 | 88 |
| Credenciales de Citación | 164 | 164 |
| Formularios | 148 | 148 |
| Base de datos de personas inscritas | 168 | 168 |
| Plataforma de inscripcio-nes | 152 | 152 |
| Sistema integrado de recaudo (SQUID) | 64 | 64 |
| TOTAL | 2167 | 2045 |

**Tabla 72. Resultado Sumatoria Valor Total Impacto del Riesgo**

Para sacar el porcentaje de la sumatoria del Valor Total Impacto del Riesgo de cada activo, se tomo la siguiente ecuación:

(Sumatoria del Valor Total Impacto del Riesgo de cada activo*100)/Sumatoria máxima del Valor Total Impacto del Riesgo de cada activo

Es decir para el primer caso (sin controles):

(2167*100)/8352 = 25.95 %

Para el segundo caso (con controles):

(2045*100)/8352 = 24.49 %

La reducción del Valor Total de Impacto del Riesgo sería:

25.95 % - 24.49 % = 1.46 %

Lo cual, con solo haber implantado 2 controles (uno en el área 2 y otro en el área 6), el riesgo se pudo reducir en un mínimo porcentaje.

Siler Amador Donado
D.N.I 72.168.640

# 6 Conclusiones, recomendaciones y trabajos futuros

## 6.1 Conclusiones

- La metodología OCTAVE-S se alinea con las directrices de la norma ISO 27005 de 2011, brindando una guía para identificar amenazas y estimar su impacto y probabilidad de manera cualitativa, sin embargo se consideró conveniente adaptarla a un método cuantitativo que permitiera medir el riesgo y visualizar la reducción de éste a medida que se ejecuta la estrategia de tratamiento del riesgo.

- Al realizar el análisis del riesgo en la seguridad de la información en DARCA con ayuda de la metodología OCTAVE-s se pudo definir a estrategia de protección y el plan de mitigación de riesgo, incluyendo los controles a implantar para realizar el tratamiento del riesgo y así ejecutar el proceso de Inscripciones y Admisiones con un nivel bajo de riesgo.

- Con la implantación de dos de los controles sugeridos para el tratamiento del riesgo, se redujo éste último un promedio de 16.97% por procedimiento y un total de reducción de 5.63% en todo el Proceso de Inscripciones y Admisiones. Se requiere de la implantación de más controles para obtener un porcentaje de reducción significativo.

- OCTAVE-S a pesar de ser una versión pequeña de la metodología OCTAVE, permite realizar un proceso de análisis y gestión de riesgo completo, cumpliendo con lo propuesto en la norma internacional ISO 27005:2011, alineándose a su vez con ISO 27002 e ISO 27001.

- La versión adaptada de la metodología OCTAVE-S producto del presente trabajo, podrá seguirse usando para realizar posteriores iteraciones de gestión de riesgos en el Proceso de Inscripciones y Admisiones de la Universidad del Cauca, aunque no queda estrictamente cerrada a dicho proceso y puede usarse como base para realizar análisis y gestión de riesgos para la seguridad de la información en otros procesos de la División

de admisiones Registro y control Académico, u otras Divisiones de la Universidad del Cauca.

### 6.2 Recomendaciones

- Cuando se requiera implantar un control, se debe tener en cuenta el costo que implica establecer dicho control, y compararlo con el valor del activo(s) que será beneficiado; es decir si el valor del activo(s) es más elevado que el valor del control se justifica su implantación.

- Se recomienda realizar mediciones periódicas en los niveles considerados de riesgo a medida que se implantan controles, esto con el fin de mantener registro de las áreas que están siendo beneficiadas y enfocar el tratamiento a las áreas que muestren mayor riesgo.

- Al seguir la metodología OCTAVE-s con un equipo de trabajo inferior a cuatro personas, se recomienda que los integrantes del equipo tengan amplia o completa información del caso de estudio y lo conozcan a fondo.

### 6.3 Trabajos Futuros

Este trabajo tuvo como principal contribución la adaptación y aplicación de la metodología OCTAVE-S al Proceso de Inscripciones y Admisiones, siguiendo las directrices propuestas en la norma ISO 27005:2011 para realizar análisis y gestión del riesgo. Así, siguiendo con las necesidades de la Universidad del Cauca, específicamente a la División de admisiones registro y control académico se proponen los siguientes trabajos futuros:

- Ejecutar el Tratamiento del Riesgo en la seguridad de la información, al proceso Inscripciones y Admisiones siguiendo la estrategia de mitigación propuesta en el presente trabajo, a través de la implantación de la mayor cantidad de controles considerados en la Declaración de aplicabilidad (SOA). Esto con el fin de llevar el riesgo en el proceso a un nivel menor.

- Construir una herramienta software de análisis y gestión de riesgos que se adapte a OCTAVE-S, y que permita hacer seguimiento continuo a los con-

troles implantados en el proceso de Inscripciones y Admisiones, generando alertas en tiempo real. Se recomienda una aplicación móvil que pueda ser usada por el encargado de seguridad informática de cada división

## 6.4 Beneficios

- ✓ Mejora de la eficacia de la Seguridad de la Información
- ✓ Diferenciación Mercado
- ✓ Proporciona confianza a los socios comerciales, las partes interesadas y clientes (certificación demuestra una diligencia adecuada)
- ✓ La única norma con la aceptación global
- ✓ tasas más bajas posibles sobre las primas de seguros
- ✓ El cumplimiento de los mandatos y las leyes (por ejemplo, la Ley de Protección de Datos, Ley de Protección de las Comunicaciones)
- ✓ Reducción de la responsabilidad debido a las políticas y procedimientos de la ONU implementadas o forzada
- ✓ Alta Dirección tiene la titularidad de Seguridad de la Información
- ✓ Norma cubre TI, así como la organización, el personal y las instalaciones
- ✓ responsabilidades del personal Enfocado
- ✓ Revisión Independiente del Sistema de Gestión de Seguridad de la Información
- ✓ Mejor conocimiento de la seguridad
- ✓ Los recursos combinados con otros sistemas de gestión (por ejemplo. SGC)
- ✓ Mecanismo para medir el éxito de los controles de seguridad
- ✓ Proporciona los medios para la seguridad de la información de gobierno corporativo y cumplimiento legal
- ✓ Enfoque conciencia de las responsabilidades del personal y crear la seguridad
- ✓ Ejecución de las políticas y procedimientos

# 7 Bibliografía y webgrafía

[1] ICONTEC, "Estándar Internacional ISO/IEC 27001:2005 Information Technology -- Securitytechniques --Specification for an Information Security Management System," ed, 2005.
[2] ICONTEC, "Estándar Internacional ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition)," ed, 2011.
[3] C. Serrano, Modelo Integral para el Profesional en Ingeniería, 2 ed. Popayán, Colombia, 2005.
[4] T. Tower, "FAIR – ISO/IEC 27005 Cookbook," ed. United Kingdom: The Open Group.
[5] P. A. Silberfich, "Análisis y Gestión de riesgos en TI ISO 27005 – Aplicación Práctica," A. O. Cruz, Ed., ed. Buenos Aires, Argentina: Segurinfo 2009 – Quinto Congreso Argentino de Seguridad de la Información, 2009.
[6] D. A. d. l. F. P. (DAFP), "Guía para la administración del riesgo," D. d. C. I. y. R. d. Trámites, Ed., 4 ed. Bogotá, D.C., 2011.
[7] M. d. C. C. Rin, "El Análisis de Riesgos dentro de una Auditoría Informática: pasos y posibles metodologías," Departamento de Informática, Universidad Carlos III de Madrid, 2013.
[8] I. N. d. T. d. l. Comunicación, "Guía Avanzada de Gestión de Riesgos," INTECO, Ed., ed, 2008.
[9] M. P. Konzen, "Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança," R. C. N. Lisandra Manzoni Fontoura, Ed., ed, 2012.
[10] P. D. P. Naranjo, "Análisis de los Riesgos y Vulnerabilidades de la Red de Datos de Escuela Politécina Nacional," Escuela de Ingeniería, Escuela Politécina Nacional, Quito, 2007.
[11] P. O. J. C. Maria Cristina Gallardo Piedra, "Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia T.I para la Empresa Eléctrica Quito S.A.," Facultad de Ingeniería de Sistemas, Escuela Politéctina Nacional, 2011.
[12] L. A. B. Torres, "Plan de Seguridad de la Información Compañía XYZ Soluciones," Universidad Autónoma de Barcelona, 2013.
[13] G. P. Mega, "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico," Instituto de Computación – Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay, 2009.
[14] I. N. d. T. d. l. Comunicación, "Implantación de un SGSI en la empresa," INTECO, Ed., ed, 2009.
[15] C. A. G. Guevara, "Establecimiento del Sistema de Seguridad de Informacion en SFG bajo los Estándares de la Norma ISO 27001: 2005," Facultad de Pstgrados, Universidad EAN, 2012.
[16] A. A. G, Diseño de un Sistema de Gestión de Seguridad de Información: Alfaomega, 2007.

[17] M. T. R. Y. S., "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN SISTEMA DE INFORMACIÓN (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO- Puerto Ordaz)," Ciencia y Tecnología, Universidad Centrooccidental Lisandro Alvarado, Barquisimeto, 2008.

[18] P. D. A. A. G., "Análisis y Evaluacion del Riesgo de Información: Un Caso en la Banca," 2006.

[19] D. H. P. Ricardo Gómeza, Yezid Donoso, Andrea Herrera, "Metodología y gobierno de la gestión de riesgos de tecnologías de la información," Agosto, 2010 2010.

[20] Z. O. B. Alexandra Ramírez Castro, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," vol. 16, pp. 56-66, 2011.

[21] J. M. M. Veiga, "Análisis de Riesgos de Seguridad de la Información," Facultad de Informática, Universidad Politécnica de Madrid, 2009.

[22] L. E. S. Antonio Santos-Olmo, Eduardo Fernández-Medina, Mario Piattini, "Revisión Sistemática de Metodologías y Modelos para el Análisis y Gestión de Riesgos Asociativos y Jerárquicos para PYMES," 2012.

[23] P. H. Ohtoshi, "Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005," Departamento de Ciência da Computação, Universidad de Brasília, Brasilia, 2008.

[24] P. P. Páez, "Aplicación de la Norma OCTAVE-S en la Empresa Pirámide Digital CIA. LTDA," ed. Quito, Ecuador, 2013.

[25] F. Soldan, "L'utilizzo di OCTAVE," in XXII Convegno Nazionale di Information Systems Auditing, ed. Parma, 2008.

Siler Amador Donado
D.N.I 72.168.640

# 8 Anexo A

## 8.1 Metodología para cumplimiento de los objetivos

| | |
|---|---|
| **1.RESPONSABLE:** | Profesional Especializado – División Admisiones, Registro y Control Académico, Estudiante TFM. |
| **2. OBJETIVO:** | Gestionar el riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S al caso de estudio: Proceso de Inscripciones y Admisiones en DARCA. |
| **3. ALCANCE:** | Inicia con la definición del alcance del caso de estudio aplicando la **Metodología de las Elipses** al Proceso de Inscripciones y Admisiones en DARCA, identificando los subprocesos y dependencias con otros procesos de la Universidad del Cauca y su interacción con entidades externas, y finaliza con la gestión del riesgo al Proceso de Inscripciones y Admisiones en DARCA con base en la adaptación de la metodología de análisis y gestión del riesgo OCTAVE-S. |
| **4. MARCO NORMATIVO:** | Reglamento estudiantil - Acuerdo 002 de 1988 modificado por el acuerdo 086 de 2008 Capítulo III |

**5. CONTENIDO**

| No. | Actividad | Descripción de la Actividad | Cargo Responsable | Punto de Control |
|---|---|---|---|---|
| **1** | Recolectar información referente al proceso Inscripciones y Admisiones | Se programa reuniones con DARCA para obtener toda la información pertinente del proceso y sus procedimientos. | Estudiante TFM | Existe información del proceso Inscripciones y Admisiones |
| **2** | Aplicar la metodología de las elipses al Proceso de Inscripciones y Admisiones, | Se organiza toda la información recolectada en la actividad anterior, identificando los procedimientos o | Estudiante TFM | Toda la información del proceso Inscripciones y Admisiones se ha recolectado |

| | | | | |
|---|---|---|---|---|
| | con el fin de definir el alcance del caso de estudio e identificar los distintos subprocesos que componen el alcance. | subprocesos del proceso Inscripcio-nes y admisiones, los responsables de manejar dichos procedimientos y las diferentes entradas y salidas que estos generan. | | |
| **3** | Identificar las distintas interacciones que los sub-procesos tienen con otros procesos de la organiza-ción | Se analiza qué otros procesos en DARCA dependen o tienen que ver con los procedimientos o subprocesos del proceso inscripcio-nes y admisiones, teniendo en cuenta todas las diferentes interacciones si existen. | Estudiante TFM | Los procedimien-tos del proceso Inscripciones y Admisiones han sido identificados |
| **4** | Identificar las organizaciones extrínsecas a la DARCA que tienen cierto tipo de inter-acción con los subprocesos identificados. | Se analiza qué otras organizaciones en la Universidad del Cauca están asocia-das o tienen que ver con el proceso y sus procedimientos, teniendo en cuenta todas las diferentes interacciones si existen. | Estudiante TFM | Los procedimien-tos del proceso Inscripciones y Admisiones han sido identificados |
| **5** | Identificar los distintos tipos de activos de información existentes dentro del alcance del modelo. | Se identifican todos los activos que entren en juego en el proceso Inscrip-ciones y Admisiones, sin descartar ninguno. | Estudiante TFM | El alcance del proceso Inscrip-ciones y Admisiones está definido |

| | | | | |
|---|---|---|---|---|
| **6** | Clasificar los activos de información según las categorías propuestas en ISO/IEC 27002. | Se procede a clasificar los activos según las categorías propuestas ISO/IEC 27002. Esto es, se clasifican en activos de tipo: información, sistemas (activos físicos), aplicaciones (activos software), servicios, personas, e intangibles. | Estudiante TFM | Los activos del proceso Inscripciones y Admisiones están identificados |
| **7** | Adaptar la metodología de análisis y gestión del riesgo OCTAVE-S al Proceso de Inscripciones y Admisiones en DARCA cumpliendo con las directrices de la norma ISO/IEC 27005 | Se contrastan las fases de OCTAVE-S con las directrices de la norma ISO/IEC 27005, teniendo en cuenta que sean aplicables al Proceso de Inscripciones y Admisiones de DARCA. | Estudiante TFM | El alcance del proceso Inscripciones y Admisiones está definido |
| **8** | Efectuar la identificación, estimación y evaluación del riesgo al Proceso de Inscripciones y Admisiones, con base en la adaptación de la metodología | Se procede a escoger los activos críticos, se analiza las diferentes áreas involucradas en el proceso identificando las falencias, estimando y evaluando tanto cualitativa como cuantitativamente | Estudiante TFM | La metodología OCTAVE-S se ha adaptado al Proceso de Inscripciones y Admisiones cumpliendo con las directrices de la norma ISO/IEC 27005 |

| | | | | |
|---|---|---|---|---|
| | de análisis y gestión del riesgo OCTAVE-S | el riesgo. Todo con base en la adaptación de la metodología de análisis y gestión del riesgo OCTAVE-S. | | |
| **9** | Desarrollar planes y estrategias de seguridad para el tratamiento y aceptación del riesgo | Se procede a determinar si se mitiga, se acepta, se transfiere, se aplaza, o se elimina el riesgo identificado en la actividad anterior. Dependiendo a eso, se desarrollan planes y estrategias de seguridad (controles) para el tratamiento del riesgo identificado. | Estudiante TFM, Profesional Especializado – División Admisiones, Registro y Control Académico | Se conoce el valor del riesgo del proceso Inscripciones y Admisiones |
| **10** | Calcular el porcentaje de reducción del riesgo, comparando el primer valor riesgo resultante, con el valor del riesgo final | Luego de haber implementado los planes y estrategias de seguridad (controles) para minimizar el riesgo del proceso, se calcula el porcentaje de reducción de dicho riesgo, comparando el valor del riesgo antes de implementar los controles, con el valor del riesgo resultante después de haber efectuado los controles. | Estudiante TFM | Los controles han sido implementados al proceso Inscripciones y Admisiones |

| | |
|---|---|
| **6. FORMATOS** | No aplica |
| **7. ABREVIATURAS Y DEFINICIONES:** | DARCA: División de Admisiones, Registro y Control Académico.<br>Metodología de las Elipses: es un método que permite identificar los distintos tipos de activos de información existentes dentro del alcance del modelo.<br>Extrínseco: Que es impropio de una cosa o es exterior a ella.<br>OCTAVE-S: Metodología de análisis y gestión del riesgo de la información.<br>Intangible: Que no puede ser tocado. |

**Gestión del riesgo con base en ISO27005 adaptando OCTAVE-S al caso de estudio.**

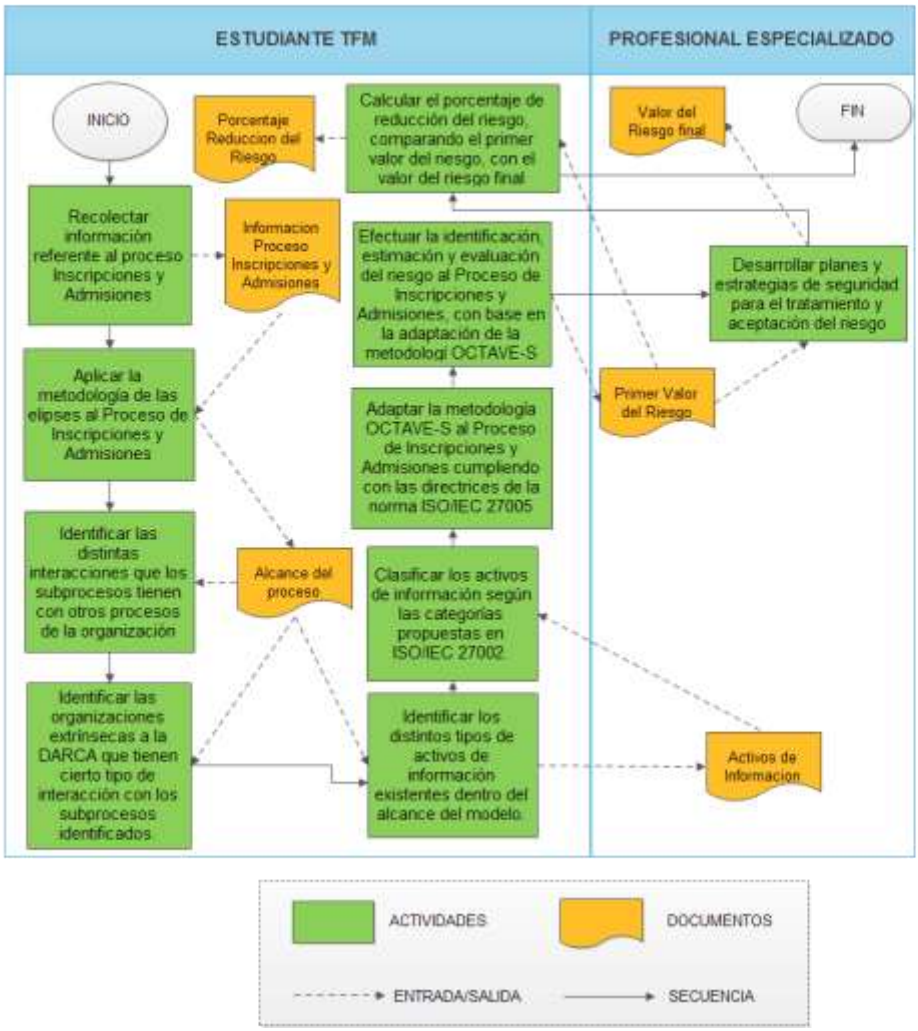


**Ilustración 12. Metodología para desarrollo de objetivos**