**ANÁLISIS DE LOS PUNTOS CRÍTICOS DE LA APLICACIÓN PROGRAM ART**

**JESSICA NATALIA PULIDO LEÓN**

**ARLINSON ESNEIDER ROJAS LUNA**

**JENNIFER ANDREA ROMANI JAMAICA**

**JUAN DAVID SABOYÁ JIMENEZ**

**CINDY JINETH SALDAÑA GUTIERREZ**

**SERVICIO NACIONAL DE APRENDIZAJE (SENA)**

**CENTRO DE DISEÑO Y METROLOGÍA**

**ANÁLISIS Y DESARROLLO DE SISTEMAS DE INFORMACIÓN**

**FICHA 683019**

**BOGOTÁ D.C.**

**2015**

**Tabla de contenido**

[OBJETIVOS 3](#_Toc428094250)

[General 3](#_Toc428094251)

[Específicos 3](#_Toc428094252)

[ANÁLISIS DE PELIGROS Y PUNTOS DE CONTROL CRÍTICOS 4](#_Toc428094253)

[Definición 4](#_Toc428094254)

[Principios del sistema HACCP 4](#_Toc428094255)

[ANÁLISIS DE LOS PUNTOS CRITICOS ENCONTRADOS EN EL PROYECTO PROGRAM ART 8](#_Toc428094256)

[1) Virus informático o código malicioso 8](#_Toc428094257)

[2) Uso no autorizado del software 9](#_Toc428094258)

[3) Robo de información 9](#_Toc428094259)

[4) Suplantación de identidad 9](#_Toc428094260)

[5) Problemas de telecomunicaciones 9](#_Toc428094261)

[6) Alteración de la información 10](#_Toc428094262)

[7) Colapse de información 10](#_Toc428094263)

[8) Utilizar código obsoleto 11](#_Toc428094264)

[9) Incendios 11](#_Toc428094265)

[10) Pérdida de la información 11](#_Toc428094266)

[11) Problemas electrónicos 12](#_Toc428094267)

[12) Errores de usuario 12](#_Toc428094268)

[13) Presupuesto 12](#_Toc428094269)

[REFERENCIAS 13](#_Toc428094270)

# OBJETIVOS

## General

* Realizar un informe que mencione los puntos críticos de la aplicación de acuerdo al análisis realizado.

## Específicos

* Definir que es Análisis de Peligros y Puntos Críticos de Control (APPCC).
* Identificar los principios del sistema HACCP.
* Realizar un análisis de peligros y puntos críticos de control en el software.
* Listar las vulnerabilidades encontradas en el análisis.

# ANÁLISIS DE PELIGROS Y PUNTOS DE CONTROL CRÍTICOS

## Definición

El Análisis de Peligros y Puntos Críticos de Control (APPCC o HACCP, por sus siglas en inglés) es un proceso sistemático preventivo para garantizar la calidad del software, de forma lógica y objetiva.



Ilustración 1: Calidad

## Principios del sistema HACCP

El Sistema de HACCP consiste en los siete principios siguientes:

**PRINCIPIO 1**: Realizar un análisis de peligros.

• Identificar los posibles peligros asociados con un proyecto en todas las fases, desde la fase de análisis hasta la implementación.

• Evaluar la probabilidad de que se produzcan peligros e identificar las medidas preventivas para su control. En este principio el equipo HACCP debe enumerar todos los peligros físicos y logicos que pueden producirse en cada fase y analizar cada uno de ellos.

**PRINCIPIO 2**: Determinar los puntos críticos de control (PCC).

• Determinar las fases operacionales que puedan controlarse para eliminar peligros o reducir al mínimo la probabilidad de que se produzcan.

• Identificar Puntos de Control Críticos (PPC) en el proceso. La determinación de un PCC en el sistema HACCP se ve facilitada por la aplicación de un árbol de decisiones.

**PRINCIPIO 3**: Establecer un límite o límites críticos.

• Establecer los límites críticos de cada uno de los PCC que aseguren que están bajo control. Este principio requiere la especificación de los límites críticos para cada medida preventiva. En ciertos casos, puede establecerse más de un límite crítico para una determinada fase. Los límites críticos son los niveles o tolerancias prescritas que no deben superarse para asegurar que el PCC es controlado efectivamente. Si cualquiera de los parámetros referentes a los puntos de control está fuera del límite crítico, el proceso se encuentra fuera de control. Por otra parte, las medidas preventivas están asociadas a esos límites críticos que funcionan como frontera de seguridad.

**PRINCIPIO 4**: Establecer un sistema de vigilancia del control de los PCC.

• Establecer un sistema de vigilancia para asegurar el control de los PPC mediante ensayos u observaciones programadas. El monitoreo o vigilancia es la medición u observación programada de un PCC en relación con sus límites críticos. Los procedimientos de vigilancia deben ser capaces de detectar una pérdida de control en el PCC. Lo ideal es que la vigilancia proporcione esta información a tiempo para que se adopten medidas correctivas con el objeto de recuperar el control del proceso antes de que sea necesario rechazar el producto. La información obtenida a través de la vigilancia o monitoreo debe ser evaluada por una persona responsable, debidamente entrenada y con el poder de decisión suficiente para aplicar medidas correctivas. El responsable de la vigilancia debe conocer la técnica de monitoreo de cada medida preventiva, entender la importancia del monitoreo, completar las planillas de registro y firmarlas.

**PRINCIPIO 5**: Establecer las medidas correctivas que han de adoptarse cuando la vigilancia indica que un determinado PCC no está controlado.

• Establecer las medidas correctivas que habrán de adoptarse cuando la vigilancia o el monitoreo indiquen que un determinado PPC no está bajo control o que existe una desviación de un límite critico establecido. Con el fin de corregir las desviaciones que pueden producirse debe formularse un plan de medidas correctivas específicas para cada PCC del programa HACCP.

**PRINCIPIO 6**. Establecer procedimientos de comprobación para confirmar que el Sistema de HACCP funciona eficazmente.

• Establecer procedimientos de verificación, incluidos ensayos y procedimientos complementarios para comprobar que el sistema HACCP está trabajando adecuadamente. Se deben establecer procedimientos que permitan verificar que el programa HACCP funciona correctamente. Se pueden utilizar métodos, procedimientos y ensayos de vigilancia y comprobación, incluidos el muestreo aleatorio y el análisis. La frecuencia de la verificación debe adecuarse a la dinámica del sistema de producción. Como actividades de verificación se pueden mencionar:

\* Examen del HACCP (sistema y responsabilidades) y de sus registros

\* Examen de desviaciones y del destino del producto.

\* Operaciones para determinar si los PCC están bajo control.

\* Validación de los límites críticos establecidos.

**PRINCIPIO 7**. Establecer un sistema de documentación sobre todos los procedimientos y los registros apropiados para estos principios y su aplicación.

• Para aplicar el programa HACCP es fundamental contar con un sistema de registro eficiente y preciso. Esto considera la elaboración de un manual que incluya la documentación sobre todos los procedimientos del programa. Así, pueden llevarse registros de:

\* Responsabilidades del equipo HACCP

\* Modificaciones introducidas al Programa HACCP

\* Descripción del producto a lo largo del procesamiento

\* Uso del producto

\* Diagrama de flujo con PCC indicados

\* Peligros y medidas preventivas para cada PCC

\* Límites críticos y desviaciones

\* Acciones correctivas.

De lo descripto hasta este punto se deduce que la clave para el buen funcionamiento de un sistema HACCP es el personal.



Ilustración 2: Principios del sistema HACCP

# ANÁLISIS DE LOS PUNTOS CRITICOS ENCONTRADOS EN EL PROYECTO PROGRAM ART

De acuerdo al análisis de peligros y puntos críticos de control en el proyecto encontramos las siguientes vulnerabilidades:

1) Virus informático o código malicioso.

2) Uso no autorizado del software.

3) Robo de información.

4) Suplantación de identidad.

5) Problemas de telecomunicaciones.

6) Alteración de la información.

7) Colapse de información

8) Utilizar código para desarrollo obsoleto.

9) Incendios

10) Pérdida de información.

11) Problemas electrónicos.

12) Errores de usuario.

13) Presupuesto.

## 1) Virus informático o código malicioso

Los virus informáticos son programas maliciosos (malwares) que “infectan” a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo “víctima” (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

## 2) Uso no autorizado del software

Delito informático que consiste en borrar, suprimir, modificar o inutilizar sin autorización datos del sistema informático, programas o documentos electrónicos almacenados en el sistema informático, con la intención de causar un daño a esos datos contenidos en las computadoras o en sistemas de redes destinados a prestar un servicio público, privado o militar.

## 3) Robo de información

Robo de información es un delito que consiste en la substracción de información para destruir o algunas veces para suplantarla y hacer robos (bancos).

## 4) Suplantación de identidad

La suplantación de identidad es un delito que puede darse en redes sociales, cuentas de correo electrónico, sistemas de nanoblogging, conversaciones telefónicas…

## 5) Problemas de telecomunicaciones

Aquellas situaciones que se presentan en cuanto a la conexión, tal caso puede ser fallos con la conexión a internet, que causaría que la aplicación no dé una respuesta pronta o simplemente no pueda ser utilizada

## 6) Alteración de la información

Entre las modalidades más comunes de alteración de la información encontramos las siguientes:

**Bomba lógica (Logic Bomb)**

Aquel software, rutinas o modificaciones de programas que producen modificaciones, borrados de ficheros o alteraciones del sistema en un momento posterior a aquél en el que se introducen por su creador. Los disparadores de estos programas puede ser desde las fechas del sistema, realizar una determinada operación o que se introduzca un determinado código que será el que determine su activación.

**Virus informático (Computer Virus)**

Se inserta una instrucción en un programa que pasa de mano en mano entre los usuarios, produciéndose el contagio entre los equipos informáticos con la consecuente destrucción de todos o parte de los sistemas con los que opera al ingresarse una determinada instrucción o en un tiempo dado, a través de la red o del intercambio de archivos.

**Piratería informática**

La piratería informática es la distribución o reproducción ilegal de las fuentes o aplicaciones de software para su utilización comercial o particular. Sea deliberada o no, la piratería informática es ilegal y está castigada por la ley.

## 7) Colapse de información

Se puede presentar cuando el sistema no posee la capacidad para guardar la cantidad de información necesaria; tal caso podría ser la base de datos que si no es actualizada estará almacenando información innecesaria y no permitirá el ingreso de nuevos datos de igual manera la creación de tablas con iguales atributos crearía redundancia de datos y estos impedirían el buen funcionamiento de la aplicación.

## 8) Utilizar código obsoleto

Es una parte del código fuente que nunca podrá ser ejecutado porque no existe ningún camino dentro de las estructuras de control en el resto del programa para llegar a este código. Es te puede ocupar memoria innecesaria y desde la perspectiva de mantenimiento de software, se pierde tiempo y esfuerzo en mantener y documentar una pieza de código que nunca se ejecuta.

## 9) Incendios

Ocurre cuando el computador o servidor no se encuentra en una sala debidamente refrigerada, también suele ocurrir cuando el cableado no se encuentra debidamente organizado, produciendo un corto circuito que genera un incendio en la sala, los incendios en estas salas también ocurren por sobre calentamiento de las maquinas.

## 10) Pérdida de la información

La pérdida de la información se genera en varios casos, como por ejemplo cuando hay un fallo en el sistema y no se cuenta con un backup de la información almacenada en este, cuando de elimina accidentalmente un archivo, cuando hay un funcionamiento anormal del sistema y algunos archivos se convierten en inaccesibles.

## 11) Problemas electrónicos

Esto sucede cuando no se cuenta con buenos dispositivos electrónicos como el hardware que se utiliza en el sistema, generando por ejemplo calentamiento conllevando al punto crítico antes mencionado como lo son incendios, también la durabilidad de estos no es buena, incrementando los costes de mantenimiento.

## 12) Errores de usuario

Estos acontecen cuando el usuario no ha sido capacitado para la utilización de un sistema, o no a leído los manuales correspondientes para saber cómo funciona este, generando el punto crítico antes mencionado como lo es la perdida de la información, generalmente ocurre con la gente que está encargada de manejar el sistema.

## 13) Presupuesto

En cualquier eventualidad que provoque que un sistema informático no se desarrolle a tiempo con el presupuesto asignado, que no atienda las necesidades del negocio ni cumpla con las expectativas del cliente, no está alineado con las metas y el contexto organizacional.

Existe un riesgo ya que los problemas financieros de la organización reducen el presupuesto del proyecto.

# REFERENCIAS

<http://es.slideshare.net/julianesteban/analisis-de-peligro-y-puntos-criticos-de-control-haccp>

<http://es.slideshare.net/guestfb90a7/sistemas-informacion-gerencial>

<https://www.infospyware.com/articulos/%C2%BFque-son-los-virus-informaticos/> <http://normatividadinformatica.bligoo.com.mx/acceso-no-autorizado-a-sistemas-de-informacion#.VbboXvkjGUs>

**Imágenes**

1) <http://2.bp.blogspot.com/-19qL4GLJwuo/UcnvP-kVuCI/AAAAAAAAAE0/_QE2EqTLsIo/s320/calidad.jpg>

2) <http://bioingenia.com/wp-content/uploads/2012/10/Picture-5.png>