MINISTERIO DE DEFENSA NACIONAL

FONDO ROTATORIO DE LA POLICIA

AUDITORIAS TECNOLÓGICAS

BASADAS EN RIESGOS

Bogota, D.C. 2020 /12 /21

Elaboró:	Revisó:	Aprobó:
Sandra A. Blanco G. **Admin. Sistemas** **Auditor**	**Economista Omar Antonio Pereira Góez** **Jefe de la Of. de Control Interno**	**Economista Omar Antonio Pereira Góez** **Jefe de la Of. de Control Interno**

TABLA DE CONTENIDO

1. Objetivo

Dar a conocer a la entidad y específicamente al área de la tecnología del Fondo Rotatorio de la Policía, aspectos relevantes que la Oficina de Control Interno de la entidad, tiene en cuenta en el momento de realizar las auditorías basada en riesgos, con el fin de que el área de telemática pueda con anticipación evaluar y actuar ante las debilidades del proceso, así como empezar a realizar los ajustes que considere necesarios en pro del mejoramiento continuo del mismo.

2. Contenido del Informe

2.1. Análisis de la situación actual del proceso tecnológico de la entidad

2.1.1. Contexto del proceso

"Actualizar, mantener y soportar el hardware y software perteneciente al Fondo Rotatorio de la Policía, apoyando tecnológicamente la operación de los procesos para la generación de productos y servicios, orientando a la entidad en la formulación de políticas, resguardando la información y realizando gestión preventiva de seguridad y salud en el trabajo y controlando los aspectos ambientales asociados"

2.1.2. Procedimientos actuales de Telemática en FORPO

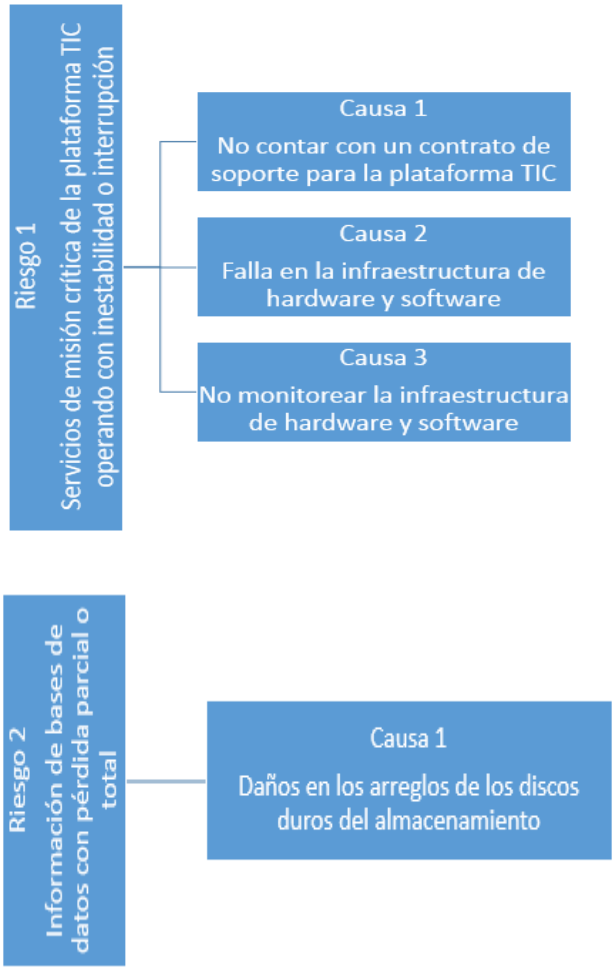
- P-3-2-01 V4 Procedimiento Administración de Plataforma de Tecnológicas de la Información y Comunicación
  - Actualizado en 20190703
  - Objetivo: "Establecer las actividades para el seguimiento de la plataforma TIC que ofrezca la disponibilidad de la misma para los usuarios finales"
  - Actividades del procedimiento
    - Levantamiento y consolidación de necesidades tecnológicas de cada una de las dependencias de la entidad
    - Presentar el plan de necesidades y Verificar las necesidades aprobadas
    - Solicitar el plan anual de adquisiciones
    - Determinar responsabilidades para el control y seguimiento de las TIC
    - Presentar estudios previos o acompañamiento en la formulación de especificaciones técnicas
    - Presentar el EDP

- Hacer seguimiento precontractual y contractual de los procesos de telemática
- Hacer seguimiento a la ejecución contractual y al comportamiento de la plataforma TIC
- Analizar las fallas, calificar el impacto y asignar los responsables del seguimiento, solución, gestión, escalamiento y evaluación para evitar nuevas ocurrencias

- P-3-2-02 V8 Procedimiento Atención de Requerimientos Telemáticos
  - Actualizado 20190703
  - Objetivo es “Definir los pasos para atender y solucionar los requerimientos telemáticos generados en el Fondo Rotatorio de la Policía”
  - Actividades del procedimiento
    - Revisar, clasificar y asignar los TAR registrados a través del software de mesa de ayuda
    - Dar solución a los requerimientos, registrar acciones y notificar al usuario
    - Verificar el estado y calificación del TAR

- P-3-2-03 V1 Gestión de incidentes de Seguridad de la Información
  - Publicado en el 20191220
  - Objetivo: “Establecer los parámetros y actividades para reportar, notificar, analizar, investigar, evaluar el impacto, escalar, aplicar las acciones definidas, recolectar información, comunicar la gestión realizada a los interesados y todas las actividades relacionadas con la gestión de incidentes con mayor impacto y recurrencia con el fin de tomar acciones para reducir la probabilidad e impacto de incidentes de seguridad de la información en el futuro
  - Actividades del procedimiento
    - Identificar y recibir notificaciones de eventos de seguridad de la información
    - Identificar, clasificar y categorizar los incidentes
    - Analizar e investigar el incidente
    - Evaluar el impacto y escalar el incidente
    - Definir y ejecutar las acciones de contención y resolución
    - Evaluación de las acciones, gestión, cierre y documentación del incidente

2.1.3. Riesgos Identificados actualmente en el proceso de Telemática - fecha de actualización 20200131



2.2. Auditorías tecnológicas basadas en riesgos

La alineación de los proyectos del Forpo debe estar enfocada al cumplimiento de la estrategia de la entidad y la tecnología es el pilar que actúa como soporte en el cumplimiento de las metas institucionales, apoyando a través de la infraestructura tecnológica de hardware y software la gestión de todas las áreas de la organización.

Teniendo en cuenta que el área tecnológica cumple un papel fundamental para la entidad, cobra gran importancia garantizar el correcto funcionamiento de cada uno de los sistemas así como el diseño, coordinación y gestión de proyectos informáticos a través de una adecuada identificación, calificación y tratamiento de los riesgos.

2.2.1. Direccionamiento de las auditorias basadas en riesgos

Las auditorías basadas en riesgos de tecnología, se direccionan en primera instancia a procesos que:

a. Tienen fallas en la identificación de la totalidad de los procedimientos del proceso
b. No han identificado las actividades de cada uno de los procedimientos
c. Carecen de identificación de la totalidad de los riesgos
d. Cuentan con un análisis débil en cuanto a la probabilidad o impacto de los riesgos detectados
e. Presentan insuficiencia en los controles para el manejo del riesgo
f. No cuentan con indicadores que midan el estado de las actividades y/o comportamiento del riesgo
g. Evidencian fallas en la toma de decisiones ante riesgos materializados, manejados únicamente a través de correcciones, sin la preparación y aplicación de acciones correctivas que impacten directamente sobre la causa-raíz
h. Carecen de acciones que demuestren la mejora continua de sus procedimientos en cuanto al análisis y documentación permanente de eventos generadores de riesgo

2.2.2. Características de los procesos maduros

Un proceso maduro evidencia:

a. Una correcta identificación de sus procedimientos, actividades, riesgos, medición y acción, por este motivo son procesos más controlados y menos suceptibles de materialización de eventos inesperados y/o tienen claramente definida la ruta en caso de presentación del mismo.
b. Realizan monitoreo constante al riesgo de sus procedimientos y/o actividades anticipándose en la medida de lo posible a situaciones que ya sea por experiencia propia o por eventos materializados en otras entidades u organizaciones son suceptibles de ocurrencia
c. Tienen claramente identificados el(los) responsable(s) y el alcance de la gestión y/o mantenimiento de los eventos de riesgo que se puedan presentar en cada procedimiento, de tal forma que no existe la posibilidad de manejar responsabilidades compartidas que dejen desprotegida a la entidad.

2.2.3. Metodología propuesta para la identificación de Procedimientos/ actividades y riesgos dentro del proceso tecnológico.

Para poder saber si se han identificado todos los procedimientos en el área de tecnología, la entidad se puede apoyar resolviendo el siguiente cuestionario:

a. Procedimientos del planear
   - Se maneja un procedimiento para la definición del Plan estratégico de TI?
   - Se cuenta con la definición de arquitectura de la información?
   - Se tiene definida la dirección tecnológica de la entidad?
   - Se definen procesos, organización y relaciones de TI?
   - Se administra la inversión de TI?
   - Se administran recursos humano de TI?
   - Se evalúan y administran riesgos de TI?
   - Se administran Proyectos?

b. Procedimientos del hacer
   - Se identifican soluciones automatizadas?
   - Se adquiere y mantiene software aplicativo?
   - Se adquiere y mantiene la infraestructura tecnológica?
   - Se adquieren recursos de TI?
   - Se administran cambios?
   - Se instalan y/o acreditan soluciones y cambios?

c. Procedimientos de Verificar
   - Se definen y administran niveles de servicios?
   - Se administran servicios de terceros?
   - Se administra el desempeño y la capacidad?
   - Se garantiza la continuidad del servicio?
   - **Se garantiza la seguridad de los sistemas**?
   - Se educa y entrenan usuarios?
   - Se administra la mesa de servicios y los incidentes?
   - Se administra la configuración?
   - Se administra el ambiente físico?
   - Se administran las operaciones?

d. Procedimientos del Actuar
   - Se monitorea y evalúa el desempeño de TI?
   - Se monitorea y evalúa el sistema de control interno?
   - Se garantiza el cumplimiento regulatorio?
   - Se proporciona gobierno de TI?

Puede ocurrir que algunos de estos procedimientos:

- no se manejen en la entidad
- se estén realizando pero no estén documentados
- estén implícitos en otros procedimientos

Realizando la identificación de actividades, se puede identificar fácilmente los riesgos relacionados al proceso, así como el control para evitar su materialización, por esta razón, se recomienda que frente a las anteriores preguntas, se identifique cuáles de ellos aplican para la entidad y para los procedimientos que aplique, verificar si se tienen contempladas las actividades y los riesgos relacionados a esas actividades

A modo de ejemplo se presentan las actividades que normalmente se realizan para el procedimiento de "**Garantizar la seguridad de los sistemas**".

- Administración de la seguridad de TI
- Plan de Seguridad de TI
- Administración de identidad
- Administración de cuentas de usuario
- Pruebas, vigilancia y monitoreo de la seguridad
- Definición de incidentes de seguridad
- Protección de la tecnología de seguridad
- Administración de llaves criptográficas
- Prevención, detección y corrección de software malicioso
- Seguridad de la red
- Intercambio de datos sensitivos

A modo de ejemplo se presentan algunos de los riesgos que podrían ocurrir en las actividades del procedimiento "**Garantizar la seguridad de los sistemas**":

- Plan de seguridad de TI que no incluya todos los requerimientos de negocio, riesgos y cumplimiento
- No contar con las inversiones requeridas en servicios, personal, software y hardware para la el cumplimiento del plan de seguridad
- Detección inoportuna de actividades inusuales en el sistema
- Inadecuada administración en aplicación de dlls y/o parches de aseguramiento del sistema
- Inadecuada clasificación de incidentes de seguridad
- Pérdida de evidencias en eventos de seguridad
- Incidentes no resueltos de manera oportuna
- Fallas para determinar oportunamente cuentas no usadas
- Falta de gestión en brechas de seguridad
- Desactualización del personal responsable en temas de seguridad

3. Conclusiones y/o Recomendaciones

3.1Conclusiones

La tecnología cambia en velocidades exponenciales, lo que exige un permanente análisis de los nuevos riesgos tecnológicos a los que se ven expuestas todas las organizaciones y así mismo se debe actuar con prontitud en el análisis de impacto y las estrategias de mitigación de los mismos, para evitar la materialización de eventos que perjudiquen los procesos de la entidad.

3.2 Recomendaciones

Realizar una autoevaluación para identificar si es necesario ajustar, modificar, establecer y/o complementar los procedimientos, actividades, indicadores, identificación de riesgos y así obtener un proceso con la madurez que evidencie el mejoramiento continuo en el área de tecnología del Fondo Rotatorio.