PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL INSTITUTO DE CASAS FISCALES DEL EJÉRCITO

2019

ELABORÓ:	REVISÓ:	APROBÓ:
ING. ATKIN ALEJANDRA TRIANA **JEFE OFICINA INFORMÁTICA**	ING. JAIRO ADRIANO ARTEAGA **ASESOR DE PLANEACION**	CR. JUAN CARLOS PARRA ARGUMEDO **DIRECTOR ICFE**

TABLA DE CONTENIDO

Tabla de contenido

1. OBJETIVO 2
2. ALCANCE 3
3. MARCO NORMATIVO 3
4. DEFINICIONES 4
5. POLITICA DE SEGURIDAD DE LA INFORMACIÓN 6
6. PLANES DE SEGURIDAD DE LA INFORMACIÓN 7
7. ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN 7
8. MARCO LEGAL 9
9. REQUISITOS TECNICOS 9
10. RESPONSABLE DEL DOCUMENTO 9

1. OBJETIVO

General:

Establecer actividades del Plan de Seguridad y Privacidad de la información para lograr establecer los primeros avances en la estructuración del Sistema de Gestión de Seguridad de la Información en el Instituto de Casas Fiscales del Ejército.

2. ALCANCE

Lograr establecer los lineamientos de fundamentación de un Sistema de Gestión de Seguridad de la Información en el Instituto de Casas Fiscales del Ejército. Este ejercicio se incluye dentro de la estrategia del Modelo de Seguridad y Privacidad de la Información del Ministerio de TIC, para lograr el cumplimiento de los requerimientos de fortalecimiento de la gestión de TI en el Estado.

3. MARCO NORMATIVO

- Constitución Política de Colombia 1991.
- Ley 87 de 1993 “Control interno en los organismos del Estado”.
- Ley 527 de 1999 “Comercio Electrónico”.
- Ley 594 del 2000 “Ley General de Archivo”.
- Ley 599 del 2000 “Código Penal Colombiano”.
- Ley 603 del 2000 “Control de legalidad del Software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la Información”.
- Ley 1273 de 2009 “Protección de la Información y de los datos”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de Junio de 2013.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
- Norma Técnica Colombiana NTC-ISO/IEC 27000
- Directiva No 2014-18 “POLITICAS DE SEGURIDAD DE LA INFORMACION PARA EL SECTOR DEFENSA”.
- Directiva Presidencial No.04 de 2012: Eficiencia Administrativa y Lineamentos de la Política de Cero Papel en la Administración Pública.
- Decreto 2573 de 2014: Por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.
- Ley 1712 de 2014: Ley de trasparencia y de acceso a la información pública nacional.
- Decreto 1078 de 2015 Artículo 2.2.5.1.2.2 : Instrumentos- Marco de Referencia de Arquitectura Empresarial para la gestión de TI LI.ES.05. Documentación de la estrategia de TI en el PETI

- Decreto 415 de 2016 Artículo 2.2.35.3: Objetivos del fortalecimiento institucional.

4. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
  - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
  - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
  - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

5. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El INSTITUTO DE CASAS FISCALES DEL EJÉRCITO ICFE se compromete con el cumplimiento de los lineamientos del Sector Defensa, preservando los atributos de confidencialidad, integridad y disponibilidad de la información, promoviendo una cultura de seguridad y administrando los riesgos de los activos de información, mediante el establecimiento, implementación, mantenimiento y mejoramiento continuo de las políticas de seguridad de la información, contribuyendo con la misión, visión y objetivos estratégicos del Instituto.

OBJETIVOS

- Proteger los recursos de información y tecnología utilizados para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el

cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos.

- Implementar un Sistema de Gestión de Seguridad de la Información, orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información en el Instituto.
- Promover, mejorar y mantener un nivel de cultura en seguridad de la información, así como lograr la concientización de todos los funcionarios y terceros que interactúan con el Instituto, para minimizar la ocurrencia de incidentes de seguridad de la información.

6. PLANES DE SEGURIDAD DE LA INFORMACIÓN

Para el presente año se pretende avanzar en los siguientes planes generales de Seguridad de la Información

1. Levantamiento de Activos de Información
2. Análisis de Riesgos de Activos de Información
3. Plan de continuidad del Negocio
4. Planes de concientización de Seguridad de la Información

7. ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN

Para el 2019 se realizarán las siguientes actividades de Seguridad de la Información teniendo en cuenta las actividades generales del área de Informática:

Actividad	Descripción	Fecha Inicial Planificada	Fecha final planificada	Responsable
Capacitación en seguridad de la información al interior de la entidad	Se plantearán temas relativos a la concientización de la seguridad de la información.	01/02/2019	31/032019	Ing. Moncada
Análisis de vulnerabilidades y seguimiento a la mitigación de brechas de seguridad en los sistemas de información.	Se realizarán las pruebas de vulnerabilidad y el seguimiento a la mitigación por parte de los administradores de sistemas.	01/02/2019	31/12/2019	Ing. Moncada

Gestión de usuarios y contraseñas	Verificar los usuarios creados definiendo los permisos y restricciones para la no manipulación de los datos almacenados en los servidores.	01/02/2019	31/12/2019	Ing. Moncada
Actualización del Registro de Bases de Datos ante la SIC	Registro de Base de Datos ICFE ante la superintendencia de Industria y Comercio	01/02/2019	31/12/2019	Ing. Moncada
Monitoreo de los sistemas de seguridad informática	Realización de informes de seguimiento del adecuado funcionamiento de las herramientas de seguridad del ICFE.	01/02/2019	31/12/2019	Ing. Moncada Informes Mensuales

8. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

9. REQUISITOS TECNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

10. RESPONSABLE DEL DOCUMENTO

Contratista en Seguridad Informática