PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2024

CONTROL DE GESTION DOCUMENTAL		
Elaboró: Ing. Andres Moncada Espitia Profesional Especializado Seguridad Informática	**Revisó y aprobó:** ASD. Dulian Paola Jiménez Gallardo Asesoría en Gestión Integral	**Aprobó:** Cr. Ernesto Mejía Araque Director Instituto de Casas Fiscales del Ejército

1. INTRODUCCIÓN

Uno de los insumos principales para la gestión, el control y la toma de decisiones del ICFE es la información que la entidad genera, almacena y administra, por tanto, es primordial establecer políticas claras y contundentes para la recolección, almacenamiento, administración y entrega de la información.

De igual modo, la tecnología es el recurso clave para el buen manejo de dicha información, la cual se desarrolla, crece y evoluciona de manera rápida y constante, requiriendo establecer lineamientos de seguridad que minimicen las alteración, fuga o indisponibilidad de la información durante las etapas de fabricación, diseño e implementación de las herramientas, incluso durante el uso de las mismas.

Por lo anterior, la entidad consolida establece las políticas en seguridad de la información para garantizar la confidencialidad, integridad, disponibilidad, no repudio y cumplimiento de las obligaciones en materia de tratamiento de datos personales, el buen uso y cuidado de la información y el funcionamiento adecuado de los recursos tecnológicos puestos a disposición de los usuarios.

Dado que la entidad cuenta con un Sistema Integrado de Gestión, este documento hace parte integral del mismo, complementando los procedimientos y guías vigentes del proceso de Tecnologías de la Información, como instrumento para orientar la implementación de la política de seguridad de la información y sensibilizar a los servidores públicos, pasantes y contratistas acerca de la importancia del buen manejo de la información.

2. OBJETIVO

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

3. ALCANCE

Este documento se proyecta como guía para el control de actividades de Seguridad de la Información de la Oficina de la Información y TIC del Instituto de Casas Fiscales del Ejército y 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.

4. NORMATIVIDAD

- Constitución Política de Colombia 1991: Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- 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: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.1377 del 27 de Junio de 2013.
- Decreto 1377 del 27 de Junio de 2013: Artículo 13. Políticas de Tratamiento de la información. Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.
- Directiva No 2014-18: Ministerio de Defensa Nacional, “Políticas de seguridad de la información para el sector defensa”, la que la modifique, aclare o adicione.
- 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 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.
- Norma Técnica Colombiana NTC/ISO 27001: La NTC ISO 27001 es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan.
- Modelo de Seguridad y Privacidad de la Información: El Ministerio TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, publica El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

5. 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.

6. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

La Entidad aprobó el Manual de Políticas de Seguridad de la Información bajo resolución interna No. 219 del 26 de diciembre de 2018, bajo la cual, 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.

6.1. OBJETIVOS DE LA POLÍTICA.

- 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.

7. PLANES DE SEGURIDAD DE LA INFORMACIÓN

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

1. Socialización del ejercicio de actualización de inventario de Activos de Información
2. Socialización del Manejo de Riesgos de Activos de Información
3. Socialización de la actualización del Plan de continuidad del Negocio
4. Actividades de concientización de Seguridad de la Información

8. ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN

En el marco de la Norma Técnica Colombiana NTC/ISO 27001 y de la Ley 1712 de 2014, la Oficina de la Información y TIC, para el año 2022 realizará las siguientes actividades de Seguridad de la Información teniendo en cuenta las actividades generales del área de Informática:

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN	DOCUMENTO O REGISTRO
1. Capacitación en seguridad de la información al interior de la entidad	Profesional en Seguridad de la Información	Se plantearán temas relativos a la concientización de la seguridad de la información, relativos a las Políticas de	Presentaciones sobre temas de Seguridad de la Información y Políticas de Seguridad

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN	DOCUMENTO O REGISTRO
		Seguridad y Continuidad de Negocio, y socialización de las amenazas inherentes al uso de sistemas informáticos en la red .	
2. Análisis de vulnerabilidades y seguimiento a la mitigación de brechas de seguridad en los sistemas de información.	Profesional en Seguridad de la Información	Se realizarán las pruebas de vulnerabilidad y el seguimiento a la mitigación por parte de los administradores de sistemas.	Informes de Análisis de vulnerabilidad
3. Gestión de usuarios y contraseñas	Profesional en Seguridad de la Información	Verificar los usuarios creados definiendo los permisos y restricciones para la no manipulación de los datos almacenados en los servidores.	Informe trimestral de avances del plan de Seguridad
4. Actualización del Registro de Bases de Datos ante la SIC	Profesional en Seguridad de la Información	Registro de Base de Datos ICFE ante la superintendencia de Industria y Comercio	Certificado emitido por el sitio web de la SIC
5. Monitoreo de los sistemas de seguridad informática	Profesional en Seguridad de la Información	Realización de informes de monitoreo de las herramientas de seguridad del ICFE(Firewall y Antivirus.	Presentación mensual de estadísticas de monitoreo de Firewall y antivirus

9. REGISTROS Y DOCUMENTOS ASOCIADOS

CÓDIGO	NOMBRE DEL DOCUMENTO
ICFE-M-10	MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

10. REGISTRO DE MODIFICACIONES (espacio exclusivo para Calidad)

VERSIÓN	FECHA MODIFICACIÓN	NUMERAL MODIFICADO	NATURALEZA DEL CAMBIO
03	13-10-2023	3 - 7	Se agrega responsable - Se actualiza marco normativo
04	20/02/2024	6	Actualización del plan para el año 2024.