Política de Seguridad de la Información y Ciberseguridad (SGSI-CIBER)

PROYECTAMOS COLOMBIA SAS

Email: gerenciatecnica@proyectamoscolombia.com

Website: https://proyectamoscolombia.com/

Proyectamos Colombia SAS

CONTENIDO

INTRODUCCIÓN

La dirección de PROYECTAMOS COLOMBIA SAS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con sus clientes, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para PROYECTAMOS COLOMBIA SAS, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI-CIBER estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de PROYECTAMOS COLOMBIA SAS
- Garantizar la continuidad del negocio frente a incidentes.
- PROYECTAMOS COLOMBIA SAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

En este sentido, PROYECTAMOS COLOMBIA SAS identifica la información como uno de los activos más importantes, ya que ésta se considera pilar para brindar sus servicios y cumplir con los objetivos propuestos. Información que se almacena, procesa y transporta en sistemas

tecnológicos que soportan la operación de los diferentes procesos; siendo vital el servicio de la plataforma tecnológica para el funcionamiento de aplicaciones internas, externas, redes y en general equipos tecnológicos que se conectan entre sí en el ciberespacio para mantener la operación de la Entidad.

El presente documento describe la Política General de Seguridad de la Información y Ciberseguridad en PROYECTAMOS COLOMBIA SAS, la cual se basa en estándares, buenas prácticas y normativas aplicables. La Política General de Seguridad de la Información y Ciberseguridad, definida y aprobada por la Junta Directiva es la base para definir la metodología de riesgos, implantación de controles y toma de decisiones de Seguridad de la Información y Ciberseguridad.

OBJETIVO

Establecer las directrices, lineamientos, responsabilidades y conductas que seguirán todos los colaboradores de la Entidad para mantener los principios de confidencialidad, integridad, disponibilidad y privacidad de la información, desarrollando habilidades y conocimientos requeridos para tener y aplicar buenas prácticas de Seguridad de la Información y Ciberseguridad, de acuerdo con las necesidades de PROYECTAMOS COLOMBIA SAS y sus clientes.

SEGURIDAD DE LA INFORMACIÓN

Seguridad de la Información, es el conjunto de medidas que tienen como fin proteger y mantener los principios de confidencialidad, integridad y disponibilidad de los Activos de Información de PROYECTAMOS COLOMBIA SAS, con el fin de prevenir incidentes tanto accidentales como intencionados, mediante la implementación de controles y medidas asociadas con las personas, los procesos y la tecnología, a la luz de las mejores prácticas y la alineación con los objetivos estratégicos de la Entidad, gestionando estrictamente el cumplimiento de obligaciones legales y regulatorias, fortaleciendo así la imagen y posición de PROYECTAMOS COLOMBIA SAS.

Principios de seguridad de la información

Para el cumplimiento de este objetivo se establecen 12 principios de seguridad que soportan el SGSI-CIBER de PROYECTAMOS COLOMBIA SAS:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- PROYECTAMOS COLOMBIA SAS protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- PROYECTAMOS COLOMBIA SAS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- PROYECTAMOS COLOMBIA SAS protegerá su información de las amenazas originadas por parte del personal.
- PROYECTAMOS COLOMBIA SAS protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- PROYECTAMOS COLOMBIA SAS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- PROYECTAMOS COLOMBIA SAS implementará control de acceso a la información, sistemas y recursos de red.

- PROYECTAMOS COLOMBIA SAS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- PROYECTAMOS COLOMBIA SAS garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- PROYECTAMOS COLOMBIA SAS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- PROYECTAMOS COLOMBIA SAS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

CIBERSEGURIDAD

Ciberseguridad, es el conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación, desarrollo, formación y buenas prácticas en general, utilizadas para prevenir y proteger los datos, sistemas y aplicaciones; salvaguardando a los consumidores financieros y activos de la Entidad en el ciberespacio, preservando los principios de la Seguridad de la Información e incluyendo las características de:

- **Control de accesos**: Proceso mediante el cual se permite o no el acceso de un usuario a aplicaciones, servidores, equipos tecnológicos entre otros, según los perfiles asignados.
- **No repudio**: Condición por medio de la cual no se puede negar la ejecución de una actividad realizada sobre la plataforma tecnológica, de acuerdo con los registros de auditoría o log's.

Principios de la Ciberseguridad

- **Mínimo privilegio**: Son todos aquellos privilegios que tienen los sistemas y aplicaciones que se encuentran interconectados pero que solo deben tener los usuarios, configuración y conexión de red necesarios para que funcionen de acuerdo con lo requerido por el proceso.
- **Mínima superficie de exposición**: Deben diseñarse las tareas o actividades a realizar en cada uno de los procesos de la Entidad, de tal forma que no queden o se habiliten canales, privilegios, IP's, usuarios, publicación o puertos que faciliten a un ciber-delincuente acceder a los sistemas, producto de estas debilidades de configuración en la red y plataforma tecnológica.
- **Defensa en profundidad**: Debe existir seguridad por niveles o anillos, es decir, que la arquitectura de red o controles de ciberseguridad que se implementen, tales como: firewall, IPS, IDS, Antivirus, WAF, antispam, honeypot, etc., deben configurarse en diferentes zonas de red. Así como usar diferentes dispositivos para dificultar el trabajo de un ciberdelincuente, obstaculizando su paso por las diferentes capas y evitando que cumpla con su objetivo.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes son los objetivos en materia de Seguridad de la Información y Ciberseguridad definidos por PROYECTAMOS COLOMBIA SAS:

- Cumplir con las obligaciones legales vigentes relacionadas con Seguridad de la Información y Ciberseguridad que apliquen a la Entidad, tomando las medidas necesarias de acuerdo con la operación que se realiza en PROYECTAMOS COLOMBIA SAS.
- Gestionar los riesgos de Seguridad de la Información y Ciberseguridad en todos los procesos de manera eficiente, con el fin de proporcionar continuidad y calidad a las operaciones del negocio.
- Facilitar la discusión al interior de la Entidad en temas de Seguridad de la Información y Ciberseguridad, ayudando a que todos los colaboradores, clientes y contratistas sean conscientes de las amenazas potenciales de Seguridad de la Información y Ciberseguridad con los riesgos asociados al negocio.
- Soportar y mejorar la calidad de las operaciones de PROYECTAMOS COLOMBIA SAS, permitiendo un equilibrio entre funcionalidad y seguridad, a la luz de las mejores prácticas de la industria.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para PROYECTAMOS COLOMBIA SAS, la información es considerada como uno de los activos importantes para el negocio y los procesos que soportan su operación, por este motivo se implementan buenas prácticas de Seguridad de la Información y Ciberseguridad que permiten cumplir con la normativa o requerimientos legales aplicables de los Entes de Control. PROYECTAMOS COLOMBIA SAS encamina los esfuerzos de los colaboradores y recurso técnico, para preservar la información y conservar la confidencialidad, integridad y disponibilidad de los activos de información, protegiendo y asegurando en el ciberespacio, los datos, sistemas y aplicaciones que son esenciales para la operación de la Entidad. Igualmente, PROYECTAMOS COLOMBIA SAS se compromete a proteger los datos sensibles, ejecutando los procesos de manera óptima y manteniendo su privacidad.

Por tanto, PROYECTAMOS COLOMBIA SAS debe:

- Establecer los fundamentos para el desarrollo y la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad, que esté alineado con la estrategia corporativa y los objetivos del negocio.
- Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad.
- Establecer que todos los colaboradores y terceros son responsables de registrar y reportar las violaciones y eventos sospechosos de Seguridad de la Información y Ciberseguridad, de acuerdo con los procedimientos correspondientes.
- Clasificar, proteger y asignar responsables de los Activos de Información, de acuerdo con la metodología que se establezca y con los criterios de valoración, en relación con la importancia que posee para la Entidad. Realizando igualmente el análisis de riesgos correspondiente, para definir los controles que preserven la información y plataforma tecnológica de la Entidad.
- Establecer los requisitos y buenas prácticas de Seguridad de la Información y Ciberseguridad, uso aceptable y controles relacionados con el acceso y utilización de los activos de la información de PROYECTAMOS COLOMBIA SAS, que mantengan y protejan las características de confidencialidad, integridad y disponibilidad de éstos.
- Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad de forma oportuna.

- Designar un equipo de Seguridad de la Información y Ciberseguridad, que se encargue de la guía, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, dando cumplimiento a la normativa.
- Definir las directrices y lineamientos relacionados con la gestión del recurso humano, para la concientización y pertenencia de la Seguridad de la Información y Ciberseguridad en todos los colaboradores.

ALCANCE DE LA POLÍTICA

La Política General de Seguridad de la Información y Ciberseguridad, así como todos los documentos de apoyo al Sistema de Gestión de Seguridad de la Información, tienen alcance a toda la Entidad, incluyendo, pero no limitado a colaboradores temporales, pasantes, terceros, personal interno y externo que tenga algún vínculo con los procesos de la Entidad, o que por motivos de negocio tengan acceso a información de PROYECTAMOS COLOMBIA SAS. Quienes tengan acceso a la información deben adoptar los lineamientos definidos por Seguridad de la Información y Ciberseguridad, cumpliendo con las políticas, normas, procedimientos y/o estándares que hayan sido definidos.

GOBIERNO CORPORATIVO

Para la aplicación y cumplimiento de la política, se establece el gobierno de Seguridad de la Información y Ciberseguridad, donde:

- La Junta Directiva Aprueba la Política General.
- El Presidente de PROYECTAMOS COLOMBIA SAS y el Comité de Seguridad de la Información, aprueban las Políticas de Dominio.
- El Oficial de Seguridad de la Información, será el responsable de la gestión y estrategia para el cumplimiento y madurez de la Seguridad de la Información y Ciberseguridad en la Entidad.
  Los líderes de área deben asumir las responsabilidades que les sean asignadas para apoyar la ejecución de las Políticas de Dominio.
- Todos los colaboradores o comunidad PROYECTAMOS COLOMBIA SAS deben cumplir con las políticas definidas.

DIVULGACIÓN DE REPORTES DE GESTIÓN

Semestralmente el Oficial de Seguridad de la Información de la Entidad, presentará a la Junta Directiva y a la Alta Dirección los resultados de la gestión realizada frente a Seguridad de la Información y Ciberseguridad.

COMPROMISO DE LA JUNTA DIRECTIVA

La Junta Directiva de PROYECTAMOS COLOMBIA SAS en cabeza de su Presidente, reconoce la importancia de identificar y proteger los Activos de Información, así como la plataforma tecnológica que soporta los procesos de la Entidad, razón por la cual evidencia su compromiso con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, apoyando el desarrollo, implementación, formalización, mantenimiento y mejora continua, que permita la mitigación de los riesgos presentes en el ciberespacio, que lleguen a afectar los datos, sistemas y aplicaciones esenciales para la operación de la Entidad.

A su vez, la Alta Dirección fortalece su compromiso evidenciándolo a través de las siguientes actividades:

- Proporcionar los recursos adecuados para el mantenimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
- Promover la cultura de Seguridad de la Información y Ciberseguridad.
- Apoyar la divulgación de las políticas y demás lineamientos de Seguridad de la Información y Ciberseguridad.
- Revisar periódicamente el Sistema de Gestión de Seguridad de la Información y Ciberseguridad para aportar al mejoramiento continuo.
- Además, de todas aquellas actividades que se encuentran consignadas en la Circula Básica jurídica expedida por la Superintendencia Financiera de Colombia que apliquen a la Alta Dirección.

En caso de cualquier violación o incumplimiento a la Política, el Comité Directivo se ocupará de la situación adecuadamente y hará todo lo posible para resolver los incidentes, diagnosticar sus causas y evitar reiteraciones.

CUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de la Política de Seguridad de la Información y Ciberseguridad es obligatorio. Cada colaborador de planta, colaborador temporal, pasante, tercero, personal interno, personal externo y contratista de PROYECTAMOS COLOMBIA SAS que tenga algún vínculo con los procesos o que acceda a la información o plataforma tecnológica de la Entidad, entenderá su rol y asumirá su responsabilidad respecto a los riesgos en Seguridad de la Información y Ciberseguridad, de acuerdo con las políticas definidas. El incumplimiento de esta Política General podrá acarrear sanciones, de acuerdo con los procedimientos establecidos para tal fin en la Entidad.

ACTUALIZACIÓN DE LA POLÍTICA

Se espera que la Política de Seguridad de la Información y Ciberseguridad se preserve en el tiempo, sin embargo, ante modificaciones por cambios en la regulación o marco legal aplicable, cambios estructurales que afecten a PROYECTAMOS COLOMBIA SAS o incidentes graves, la política debe ser revisada y/o modificada y estos cambios aprobados por la Junta Directiva de PROYECTAMOS COLOMBIA SAS

IMPLEMENTACIÓN DE LA POLÍTICA

La Política General de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad integrado en el día a día de la operación de la Entidad. Como sistema de gestión, debe tener una madurez continua, para alcanzar los objetivos establecidos en el presente documento. Se anticipa y autoriza el desarrollo de políticas de dominio, normas, procedimientos, estándares, guías, instructivos que serán publicados en el aplicativo de Administración del SIG y otras medidas administrativas que sean necesarias incluyendo la definición de una unidad o grupo de Seguridad de la Información y Ciberseguridad, así como el desarrollo o la adquisición de las herramientas, software y demás recursos que se requiera como apoyo a la gestión realizada.

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad se desarrolla con base en las siguientes etapas:

- **Prevención**: PROYECTAMOS COLOMBIA SAS desarrolla e implementa controles para velar por la Seguridad de la Información y la gestión de la Ciberseguridad, que permiten evitar incidentes sobre la información o plataforma tecnológica.
- **Protección y detección**: PROYECTAMOS COLOMBIA SAS implementa controles y actividades de monitoreo que permiten identificar eventos de Seguridad de la Información y Ciberseguridad, para tener una detección temprana que permita tomar acciones de contención o realizar la gestión que corresponda para atender los eventos evitando que estos se conviertan en incidentes.
- **Respuesta y comunicación**: PROYECTAMOS COLOMBIA SAS establece planes de respuesta a incidentes de Seguridad de la Información y Ciberseguridad, para proceder a ejecutar actividades de análisis y contención, incluyendo la comunicación, en caso de ser necesario el apoyo de entes externos como por ejemplo el CSIRT del Gobierno o COLCERT.
- **Recuperación y aprendizaje**: PROYECTAMOS COLOMBIA SAS define las actividades que permiten restaurar los servicios afectados por un incidente de Seguridad de la Información o Ciberseguridad, documentando posteriormente las lecciones aprendidas para identificar debilidades en controles, como se desarrolló el ataque, afectación y mejoras que puedan aplicarse a los planes de respuesta a incidentes.

ANTECEDENTES NORMATIVOS

El marco Normativo aplicable a PROYECTAMOS COLOMBIA SAS en asuntos relacionados con Seguridad de la Información y Ciberseguridad, el cual es la base de la implementación del Sistema de Gestión se presenta a continuación:

- Circular Básica Jurídica de Superintendencia Financiera de Colombia.
- Ley 23 de 1993 y Ley 44 de 1993: Derechos de autor.
- Ley 679 de 2001 y Ley 1336 de 2009: Pornografía Infantil.
- Ley 1266 de 2008: Habeas Data.
- Ley 1273 de 2009: Delitos Informáticos.
- Ley 201 de 2012: Ley TLC.
- Ley 1581 de 2012: Protección de datos personales.
- Circular Externa 042 de 2012: Capitulo décimo segundo: Requerimientos mínimos de seguridad y calidad para la realización de operaciones.
- Circular Externa 007 de 2018: Requisitos mínimos para la gestión de riesgos de Ciberseguridad.

Además, sienta las bases del cumplimiento de las siguientes normativas:

- ISO/IEC 27001:2013 Information technology--Security techniques--Information security management systems - Requirements.
- ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls.

CONTROL DE VERSIONES

Última revisión: Junio 2021

- Creado en Julio 2020 por la Gerencia Técnica.