POLITICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO GENERAL

Establecer la política de seguridad de la información para asegurar la confidencialidad, integridad y disponibilidad de los activos de información de los diferentes procesos de PROYECTOS REO S.A.S., teniendo en cuenta los requisitos legales vigentes.

2. OBJETIVOS ESPECIFICOS

- Proteger los activos de la información de PROYECTOS REO S.A.S. mediante la implementación de la presente política, procedimientos y controles de seguridad requeridos.
- Prevenir, identificar y gestionar los posibles incidentes de seguridad que llegaren a presentar al interior de la organización y que puedan atentar contra la confidencialidad e integridad de los activos de información.
- Adoptar una cultura de seguridad de la información por parte de los colaboradores de la empresa.

3. ALCANCE DE LA POLITICA

La política de seguridad de la información es aplicable en todo el ciclo de vida de los activos de la información de la empresa, incluyendo su creación, distribución, almacenamiento y destrucción. De igual forma es aplicable para todos los colaboradores, contratistas o terceros que pudieran llegar a desempeñar alguna labor en la empresa y que fueran conocedores de los activos de información.

4. SEGURIDAD DE LA INFORMACION

PROYECTOS REO S.A.S. converge en adoptar niveles de seguridad y protección de los activos de información a través de los recursos tecnológicos y humanos con el fin de evitar la pérdida, mal uso, alteración o acceso no autorizado y robo de la información en la protección, preservación y administración de la confidencialidad, integridad y disponibilidad de sus activos de información.

PROYECTOS REO S.A.S., asume el compromiso de implementar la política de seguridad de la

información para proteger los activos de la información de cada uno de los procesos y áreas de la empresa comprometiéndose a:

- Implementar políticas de seguridad y complementarios para asegurar la confidencialidad, integridad y disponibilidad de los activos de información empresarial.
- Implementar controles físicos y digitales orientados a la prevención de incidentes de la seguridad de la información.
- Fomentar la cultura y toma de conciencia entre el personal (colaboradores, contratistas, clientes, proveedores, terceros) sobre la importancia de la seguridad de la información.
- Definir las responsabilidades frente a la seguridad de la información.
- Proteger la información generada, procesada, resguardada o tratada de manera física o digital por parte de los procesos y áreas de la empresa.
- Mitigar los incidentes de seguridad y privacidad de la información de forma eficiente y eficaz con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas y/o activos de información.
- Garantizar el cumplimiento de las obligaciones legales regulatorias y contractuales establecidas.

5. ACUERDOS DE CONFIDENCIALIDAD.

Todos los colaboradores, contratistas, proveedores y terceros que deban realizar ejercicio de labores dentro de la empresa ya sea por medios tecnológicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el acuerdo de confidencialidad de la información.

Cuando se tenga acceso a la información de PROYECTOS REO S.A.S. se está obligando a la aceptación formal de la reglamentación de acceso y tratamiento de la información que definan las leyes de Colombia, acuerdos internacionales suscritos por Colombia, normas del sector, políticas, estándares o cualquier tipo de control establecido para la protección o tratamiento de la información.

6. DEBERES DE LOS USUARIOS DE LA INFORMACIÓN

- Respetar la confidencialidad de la información de la empresa.
- Usar la información de PROYECTOS REO S.A.S. únicamente para propósitos relacionados con el objeto social de la empresa y en cumplimiento de sus actividades o funciones.
- Ajustarse a las directrices de clasificación de la información.
- No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial.
- No anotar y/o disponer en lugares visibles las contraseñas de acceso a los sistemas de

información.

- Bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.
- Las impresiones deben de ser recogidas al momento de ser generadas.
- Devolver y no conservar ningún tipo de copia de los activos de información una vez termine la relación contractual con la empresa.
- Se prohíbe la divulgación, cambio, retiro o pérdida no autorizada de la informacion de la empresa almacenada en medios físicos removibles como USB, CD etc.
- Se prohíbe utilizar software no licenciado en los recursos tecnológicos de la empresa.
- Se prohíbe copiar software de la empresa o dispuesto por el cliente para utilizar en equipo de cómputo personal dentro o fuera de las instalaciones de la empresa.
- Todos los colaboradores, contratistas y terceros que presten sus servicios a la empresa deben aplicar todos los controles de seguridad definidos por PROYECTOS REO S.A.S para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades o que por otras situaciones esté bajo su custodia.

7. DEBERES DE LOS RESPONSABLES DE PERSONAL (COORDINACION ADMINISTRATIVA)

- Conceder autorizaciones de acceso a la información de acuerdo con las funciones y actividades propias del cargo del colaborador.
- Restringir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.
- Ser el responsable de conocer, solicitar y ratificar los privilegios de acceso a los colaboradores que le reportan.
- Mantener actualizadas las autorizaciones y perfiles de usuario basándose en las políticas de la empresa, los roles y perfiles del cargo.
- Los contratos que se suscriban con terceros deberán de detallar los acuerdos relacionados con la propiedad de la información y la no divulgación de la información confidencial.
- Cuando un empleado se ausenta de su trabajo por un mediano periodo de tiempo bien sea por licencias, incapacidades u otras situaciones, se deberá determinar lo siguiente:

  - Sí los accesos a los recursos físicos y a la información deben ser suspendidos. En caso de que ello ocurra, se deberá de notificar la fecha en que el acceso debe ser suspendido, de ser necesario, recoger los equipos de seguridad como por ejemplo llaves, claves, computadoras, etc.
  - Comunicar a las partes interesadas dichas situaciones.

  Cuando el colaborador es retirado del cargo se deberá:

  - Revocar las autorizaciones.
  - Revocar o restringir los privilegios de acceso.
  - Recoger los equipos, los dispositivos físicos y la revocación de las autorizaciones a los

sistemas de información.
- Comunicar a las partes interesadas dichas situaciones.

8. INFORMACION CONFIDENCIAL

- Para poder almacenar, recolectar, difundir, tratar, la información confidencial, se deberá de tener la autorización del titular de la información.
- La divulgación cualquiera que fuere su medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla de acuerdo a las funciones de quien la trate, respetando siempre los derechos de acceso de la información.
- El acceso o distribución de información de uso interno debe estar limitado a empleados u otros con la necesidad de conocerla o usarla para el cumplimiento especifico de sus funciones.
- Documentos que contengan información confidencial deben ser impresos en un área segura.
- Los documentos con esta información no pueden ser dejados en lugares inseguros y tampoco pueden ser desatendidos
- Acceso a información confidencial que se encuentre almacenada debe ser adecuadamente controlado.
- Las copias de respaldo de informacion confidencial deben ser protegidas de destrucción intencionada o accidental.
- Información almacenada por periodos prolongados debe ser revisada regularmente para verificar su legibilidad
- Estas políticas aplican tanto a los originales como a todas las copias de la información.

9. USO ADECUADO DE LOS EQUIPOS DE COMPUTO

- PROYECTOS REO S.A.S. sólo puede utilizar software desarrollado, adquirido legalmente o dispuesto por sus clientes
- La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas, se realizará conforme a las necesidades determinadas por la empresa.
- Los colaboradores deben cumplir con la regulación que protege los derechos de autor.
- Los equipos de cómputo deben mantener activo un software antivirus, Sistema Operative, Microsoft Office, licenciados y actualizados.
- Los computadores deben ser analizados contra virus periódica y automáticamente.
- Es responsabilidad de los colaboradores reportar todos los incidentes de infección de virus a la coordinación administrativa.
- Es responsabilidad de los colaboradores tomar copias de la información y verificar que el respaldo esté libre de cualquier infección de virus.
- Los colaboradores deben asegurar que toda la información provenga de fuentes conocidas y confiables.

10. CONTROL DE CONTRASEÑAS.

- Los perfiles de usuario y la contraseña son asignados por la coordinación administrativa o el jefe inmediato.
- Los colaboradores no pueden informar su contraseña a otros miembros de su equipo de trabajo o de otros procesos.
- Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente.

11. COPIAS DE RESPALDO DE INFORMACION

- Se debe contar con un sistema automatizado para las copias de respaldo.
- Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
- Los colaboradores son responsables por respaldar la información, y por facilitar la oportuna restauración de la información.
- Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.

12. MANEJO DE ACTIVOS DE INFORMACIÓN

Toda persona que realice actividades para PROYECTOS REO S.A.S. (colaborador, contratista) debe tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas, de conformidad con el principio de “necesidad de conocer para para realizar la actividad”.

• Todo acceso a la información debe cumplir con los requisitos legales, normativos, reglamentarios, procedimentales o de cualquier otra índole que haya definido PROYECTOS REO S.A.S.

• Todo acceso a la información debe ser autorizado formalmente por la coordinación administrativa. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.

• La información es uno de los activos más valiosos de la empresa, es por esa razón que todos los funcionarios y contratistas que prestan sus servicios en PROYECTOS REO S.A.S. se deben comprometer a realizar sus mejores esfuerzos para aplicar todos los controles de seguridad de la información definidos por el sistema de gestión de seguridad de la información de empresa, para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades.

• Todos los funcionarios y contratistas de la empresa deben reportar sin demoras injustificadas a los responsables de sus áreas, a los responsables de los procesos, la coordinación administrativa o al oficial de seguridad de la información cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información de la empresa.

- Los responsables de proceso y áreas de la empresa deben generar y conservar un registro detallado de todos los eventos que sucedan sobre los diferentes activos de información su cargo.

- Todos los colaboradores de la empresa deben aplicar los controles de seguridad de la Información definidos el sistema de gestión de seguridad de la información para reducir los riesgos que afectan a la seguridad de la información.

- Todos los colaboradores de la empresa se comprometen a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está sometida la empresa para la protección de la información a su cargo.

12.1 MANEJO DE DOCUMENTOS Y/O INFORMACIÓN ELECTRONICA

El servicio de correo electrónico institucional debe ser utilizado únicamente para las tareas propias de la función desarrollada por la empresa en cumplimiento de su objeto social, los usos diferentes a los necesarios para el cumplimiento de las funciones encargadas al colaborador, contratista o tercero son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio.

Este medio se puede utilizar para enviar adjuntos como cartas, memorandos, circulares y cualquier otro documento que sea necesario para la sustentación del contenido, razón por la cual, para garantizar el éxito en el intercambio del correo electrónico, se presentan las siguientes sugerencias:

- Se recomienda que el saludo y la despedida sean como una carta normal.
- Se sugiere escribir el mensaje, teniendo en cuenta las reglas básicas de ortógrafa (tildes, mayúsculas. diéresis, puntuaci6n, entre otros).
- Antes de contestar un mensaje se deberá tener en cuenta lo que se va a contestar y lo que es necesario para entender el contexto del mensaje.
- Se aconseja incorporar una firma al final de cualquier mensaje, donde se incluya el cargo, la organización, el proceso, el teléfono y la extensión.
- No se recomienda utilizar las letras mayúsculas.
- Se recomienda utilizar el campo con copia oculta (CCO), cuando se envíe o se responda un mensaje que incluya múltiples direcciones, o cuando se envíen mensajes que incluyan muchas personas o grupos corporativos. Esto con el fin de no publicar las direcciones de correo
- Se recomienda ser breve.
- Se debe tener cuidado con los archivos adjuntos, se recomienda no adjuntar archivos con virus o con un archivo que no pueda recibir o descargar el destinatario.
- Los colaboradores deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad la empresa.
- Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los colaboradores podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera comprimida y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.
- Las comunicaciones electrónicas en lo posible deben ser concretas, precisas y completas.

- Los Comunicados Generales son comunicados emanados desde la coordinación administrativa hacia la totalidad de los colaboradores.
- La asignación de correo electrónico a los colaboradores será realizada por la coordinación administrativa.
- No deberá de utilizarse correo electrónico corporativo para trámites personales.
- Los mensajes de correo salientes deben de llevar campo en el asunto, que referencie la temática del contenido del texto.
- La confirmación de lectura sólo se utilizará en situaciones estrictamente necesarias.
- Antes de enviar un correo deberá verificarse que este dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades.
- El manejo de documentos electrónicos es transversal a todos los procesos de la empresa.
- La clave de acceso al servicio de correo electrónico no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por PROYECTOS REO S.A.S.
- Al finalizar su relación laboral todo colaborador, contratista o tercero que preste sus servicios a PROYECTOS REO S.A.S., debe realizar la devolución de la cuenta de usuario de correo electrónico al responsable del proceso para el cual labora.
- Como lo establece el artículo 13 de la Constitución Política de Colombia “Todas las personas nacen libres e iguales ante la ley, recibirán la misma protección y trato de las autoridades y gozarán de los mismos derechos, libertades y oportunidades sin ninguna discriminación por razones de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica.”, por lo anterior el uso del correo electrónico para comunicaciones personales o institucionales no debe:
  - Difundir mensajes que promuevan, induzcan o inciten a la discriminación de las personas en razón a sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica.
  - Usar el correo institucional con fines diferentes al cumplimiento de las funciones asignadas, por ejemplo: difusión avisos clasificados o publicidad comercial no deseada o beneficio personal.
  - Como lo establece la Ley 1273 de 2009, está prohibida la Interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, por lo que está prohibida la interceptación de los mensajes de correo electrónico sin autorización legal.
  - Como lo establecer la Ley 1273 de 2009, está prohibido el acceso abusivo a un sistema informático, por lo tanto, está prohibido acceder al buzón de correo electrónico de otros colaboradores sin la debida autorización.
  - Crear, almacenar o intercambiar de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales

12.2 MANEJO DE DOCUMENTOS Y/O INFORMACION FISICA

- El ingreso a las instalaciones PROYECTOS REO S.A.S. debe estar restringido únicamente al personal autorizado.
- El registro de visitantes debe incluir el nombre e identificación del visitante, la fecha y hora de entrada y salida del visitante.
- El acceso a los centros de datos debe ser restringido y sólo pueden ingresar personal autorizado por la coordinación administrativa.
- Los privilegios de acceso físico a los centros de datos de los colaboradores autorizados deben ser eliminados a la terminación de la vinculación laboral o contrato laboral, o por alguna novedad.
- Ningún activo de información físico se debe retirar de las instalaciones de la empresa sin autorización del responsable del activo. La solicitud del retiro del activo debe ser realizada por los líderes del proceso y autorizada por la coordinación administrativa.
- En la disposición, archivo, trasferencia de documentos deben considerarse todas las medidas que garanticen la conservación del material, tales como la manipulación, embalaje y transporte, entre otras, y aquellas que eviten la contaminación y propagación de factores nocivos y accesos no autorizados.
- La coordinación administrativa debe implementar controles para garantizar que los archivos de gestión de la empresa cuenten con los mecanismos de seguridad que salvaguarden y conserven dicha información.

13. PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES

Se debe de asegurar la privacidad y la protección de la información de datos personales, como se exige normatividad legal vigente, cuando sea aplicable. PROYECTOS REO S.A.S. tiene definida una política de tratamiento de datos personales, siendo el Oficial de Protección de Datos Personales el responsable en materia de seguridad de la información de:

- Adelantar las investigaciones necesarias por las posibles violaciones a las normas legales vigentes de protección de datos personales.
- Velar por la implementación de planes de auditoría para verificar el cumplimiento de las Políticas y Procedimientos en materia de Protección de Datos Personales.
- Velar porque se capacite periódicamente en temas de protección de datos personales a los colaboradores, para generar una cultura de protección de datos dentro de la empresa.
- Integrar la Política de Tratamiento de Datos Personales dentro de las actividades de las demás áreas de la empresa.
- Apoyar la construcción de reglas sobre el uso responsable de la información, incluyendo controles de seguridad administrativos, físicos, tecnológicos, lógicos y jurídicos.
- Realizar los reportes de incidentes de seguridad en el RNBD conforme a los parámetros establecidos en la Ley 1581 de 2012 y demás normas concordantes y vigentes.

14. SEGURIDAD DE LA INFORMACION DATO SENSIBLE

Los datos personales sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Toda persona que realice actividades para PROYECTOS REO S.A.S. (colaborador, contratista) debe tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas, más aún si se trata de información sensible, el cual, podrá realizar su tratamiento de manera exclusiva cuando se cuente con la respectiva autorización del titular del dato personal o cuando sea necesaria para la defensa de un derecho fundamental del titular o cuando haya sido requerida por autoridad judicial o administrativa en el curso de un proceso o actuación judicial.

Para el tratamiento de los datos sensibles del titular de la información, se deberán de tener en cuenta todos los lineamientos que se han establecido en el presente documento, lo referente al manejo de la informacion física y electrónica, copias de respaldo de la informacion, control de contraseñas, uso adecuado de los equipos de cómputo, información confidencial, deberes de los responsables del dato personal, deberes de los usuarios de la información, acuerdos de confidencialidad y en general todo lo relacionado con el manejo de activos de la información.

15. PROPIEDAD INTELECTUAL

Todo el material que es desarrollado por una persona que tenga una vinculación como colaborador o como contratista de PROYECTOS REO S.A.S., se considera que los derechos patrimoniales son propiedad de la empresa y que es de uso exclusivo de la misma, por lo tanto, debe ser protegida contra un develado, descubrimiento o uso que menoscabo los intereses empresariales, misionales, reputacionales, económicos y en general cualquier perjuicio contra PROYECTOS REO S.A.S., en los términos de la ley 23 de 1982 y sus normas reglamentarias y aquellas que la modifiquen.

La coordinación administrativa debe de realizar las tareas pertinentes para que, en los contratos suscritos con colaboradores, contratistas, y/o terceros se incluyan las cláusulas correspondientes que especifiquen los compromisos y cuidados que se debe tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad. Con el fin de cumplir las leyes sobre propiedad intelectual, se deben de adelantar acciones para el guardado de archivos dentro de los equipos de la empresa y en ese sentido, generar procesos para el borrado de archivos que no deban estar en los computadores, tales como archivos de video (mp4, avi, flv, etc.), archivos de audio (3gp, mp3, etc.), fotografías, etc. Hay que tener en cuenta que ciertos colaboradores deben estar dentro de las excepciones, toda vez que el cumplimiento de sus funciones está orientado a la producción de dicho material, caso en el cual se debe documentar y adelantar las solicitudes correspondientes para poner en firme dicha excepción.

16. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Esta política establece los lineamientos generales para reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo durante o fuera de las horas laborales de la empresa. Aplica a colaboradores, contratistas y terceras partes que por la naturaleza de sus funciones deban tener acceso a estaciones de trabajo o puestos de trabajo dentro de las instalaciones de PROYECTOS REO S.A.S.

Con la presente Política de Seguridad y Privacidad de la Información es clara la declaración general que representa la posición de la administración de PROYECTOS REO S.A.S. con respecto a la protección de los activos de información *(los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software),* que soportan los procesos de la empresa y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Esta política aplica a toda la entidad, sus colaboradores, contratistas y terceros de PROYECTOS REO S.A.S, por lo tanto, todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la presente política.

JOSE OSCAR ZULUAGA HERRERA

Representante Legal
Marzo 12 2024