PROYECTAMOS SAS

Manual de Políticas de Seguridad de la Información



Proyectamos Colombia SAS

CONTENIDO

INTRODUCCIÓN 2
OBJETIVO..... 3
DEFINICIONES 4
LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN 8
LINEAMIENTOS DE PRIVACIDAD 9
LINEAMIENTO DE ROLES Y RESPONSABILIDADES 10
LINEAMIENTOS PARA EL USO DE DISPOSITIVOS MÓVILES..... 12
SEGURIDAD DE LOS RECURSOS HUMANOS..... 14
LINEAMIENTOS PARA EL USO DE CORREO ELECTRÓNICO 17
LINEAMIENTOS PARA EL USO DE INTERNET 21
LINEAMIENTOS PARA LOS SISTEMAS DE MENSAJERÍA INSTANTÁNEA 23
LINEAMIENTOS DE USO DE REDES SOCIALES..... 24
LINEAMIENTOS PARA EL USO DE RECURSOS TECNOLÓGICOS..... 25
LINEAMIENTOS RELACIONADOS CON LA CLASIFICACIÓN, CONTROL Y PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN 27
LINEAMIENTOS PARA LA GESTION DE MEDIOS DE ALMACENAMIENTO 31
LINEAMIENTOS RELACIONADOS CON EL CONTROL DE ACCESO ... 33
LINEAMIENTOS DE LA SEGURIDAD FÍSICA Y DEL ENTORNO 36
LINEAMIENTOS DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA 39
LINEAMIENTOS PARA LA GESTIÓN DE CAMBIOS 40
LINEAMIENTOS RELACIONADOS CON LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE 41
LINEAMIENTOS PARA LA SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN..... 43
LINEAMIENTOS PARA PROTECCIÓN CONTRA CÓDIGO MALICIOSO44
LINEAMIENTOS DE BACUP..... 46
LINEAMIENTOS DE EVENTOS DE AUDITORÍA..... 51
LINEAMIENTOS PARA LA GESTIÓN DE SEGURIDAD DE LAS REDES 52
LINEAMIENTOS PARA EL INTERCAMBIO DE INFORMACIÓN..... 55
LINEAMIENTOS PARA EL MANEJO DEL REGISTRO DEE ACTIVIDADES56
LINEAMIENTOS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 57
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES 59
POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 60
LINEAMIENTOS PARA LA PROTECCIÓN DE LOS DERECHOS DE AUTOR Y LICENCIAMIENTO 61
CONTROL DE CAMBIOS 63

INTRODUCCIÓN

La dirección de PROYECTAMOS 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.

El Desarrollo de este manual es basado en el Modelo de Seguridad de y Privacidad de la Información expuesto por el Ministerio de la Tecnologías de la Información y las comunicaciones, el cual recopila las mejores prácticas para suministrar requisitos para el diagnóstico, planificación, implementación, Gestión y mejoramiento continuo; lo anterior teniendo en cuenta las necesidades y objetivos, los requisitos de seguridad, los procesos misionales de PROYECTAMOS SAS.

Lo que se pretende es lograr la preservación de la confidencialidad, integridad y disponibilidad de la Información, garantizando la privacidad de los datos mediante la aplicación de la Gestión del Riesgo.

De esta forma estamos dando cumplimiento al decreto único reglamentario 1078 de 2015 en el componente de seguridad y privacidad de la Información como parte integral de la estrategia GEL.

El modelo a seguir está basado en las Normas Técnicas NTC ISO/IEC 27000 y las ISO/ICONTEC, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otros. Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Las políticas incluidas en este manual se convierten en la base para implementar controles en la Información misional de PROYECTAMOS SAS.

OBJETIVO

Establecer los lineamientos procedimentales basado en las Políticas en Seguridad de la Información y ciberseguridad de Proyectamos SAS, de acuerdo con los lineamientos de buenas prácticas en Seguridad, Privacidad para el manejo y protección de la información física y lógica propia y de terceros, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

DEFINICIONES

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Acuerdos de Niveles de Servicio ANS:** es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Autorización de usuarios:** Todos los usuarios deben ser identificados independientemente, con permisos de accesos específicos e individuales. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización específica de acuerdo con las funciones de los usuarios y auditoria confiable.
- **Confianza:** Los proveedores de productos y/o servicios de TI deben demostrar capacidad para reunir o exceder los requerimientos de seguridad la información, y justificar la confianza en sus capacidades para asegurar los activos de información de PROYECTAMOS SAS. La confianza empieza a ser incrementalmente importante cuando activos de información sensibles son compartidos con otras entidades y proveedores de servicios.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Copias de respaldo o Backup:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
- La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen
- **Información Pública reservada:** información que estando en poder y custodia es exceptuada de acceso por daño de intereses públicos.
- **Información Pública Clasificada:** información cuyo acceso podrá ser rechazado o denegado siempre que cause daños a:
  - Intimidad
  - Vida
  - Salud o seguridad
  - Secretos comerciales, industriales o profesionales
- **Instructivo:** Documento que describe de una manera detallada cómo debe ejecutarse una actividad o tarea determinada para garantizar su realización, hablan sobre métodos específicos sobre plataformas, sistemas de información o algún proceso definido.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Licencia de software:** es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **Logs:** Grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema.
- **Mensajería Instantánea:** Es una forma de comunicación en tiempo real entre dos o más personas basada en texto.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

- **Propiedad de la información:** Los activos de información son propiedad de la PROYECTAMOS SAS y son entregados para su uso, operación o custodia a los funcionarios, contratistas y terceros, de acuerdo con la función específica y necesidades del trabajo a realizar, aunque dentro de las funciones específicas se nombre dentro del ciclo de vida del activo de información u operación un propietario de cada activo. Este nombramiento como propietario, se hará únicamente, con el fin de asignar las responsabilidades operativas y de custodia sobre los diferentes activos.

- **Protección de la información:** Los activos de información serán protegidos con el nivel necesario, en proporción a su valor y al riesgo de pérdida de PROYECTAMOS SAS. La protección debe propender por la confidencialidad, integridad y disponibilidad del activo de información.

- **Protección de los recursos tecnológicos:** Los recursos tecnológicos de PROYECTAMOS SAS serán protegidos con el nivel necesario en proporción a su valor y a los riesgos a los que puedan estar expuestos. Dichos recursos deben ser utilizados exclusivamente para desarrollar actividades laborales y así mismo su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

- **Responsabilidad:** Los usuarios y custodios de los activos de información en PROYECTAMOS SAS son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas en la PROYECTAMOS SAS generarán y mantendrán unas apropiadas pistas de auditoría para identificar usuarios, y documentar los eventos relacionados con la seguridad.

- **Revisiones de seguridad en sistemas de Información:** Se deberán tener habilitados diferentes criterios para verificar el cumplimiento de los estándares de configuración de seguridad de la información en las diferentes plataformas técnicas e instalaciones de tecnología de información.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Servidor (hardware):** un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software.
- **Servidor (software):** un servidor basado en software es un programa que ofrece un servicio especial que otros programas denominados clientes pueden usar a nivel local o a través de una red.
- **Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Usuario:** Se denomina usuario al funcionario, Contratista o Tercero al cual se le ha dado acceso a los servicios de tecnología de la Entidad.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Dando cumplimiento a las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información en la PROYECTAMOS SAS, se elaboran una serie de lineamientos que se describen a continuación:

PROYECTAMOS SAS se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la visión y misión de la entidad. Las responsabilidades para la gestión de la seguridad de los activos de información deben estar claramente asignadas en todos los procesos y subprocesos de la entidad.

El cumplimiento de todos los requisitos de ley y de los organismos de control debe ser presentados y aprobadas por los líderes con el fin de proveer un ambiente seguro y estable de recursos de información que sea consistente con las metas y objetivos de PROYECTAMOS SAS. Todos los funcionarios, contratistas y terceros con acceso a los activos de información de PROYECTAMOS SAS se hacen responsables de cumplir con el lineamiento de seguridad de la información La Dirección General se compromete a velar por la aplicación y cumplimiento adecuado de los siguientes lineamientos de seguridad y privacidad de la información y todas las que se deriven de ella, por parte de todos los funcionarios, contratistas y terceros vinculados a PROYECTAMOS SAS. La Entidad se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar los riesgos a un nivel aceptable. Establecer la mejora continua del Subsistema de Gestión de Seguridad y Privacidad de la Información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de PROYECTAMOS SAS, de una manera contundente, eficiente y efectiva, de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo a la metodología adoptada por la Entidad.

LINEAMIENTOS DE PRIVACIDAD

PROYECTAMOS SAS respeta la privacidad de la información; Al procesar los datos personales se está dando cumplimiento estricto a lo establecido en la Ley 1581 de 2012 reglamentada de forma parcial en el Título II, Capítulo 25 del Decreto 1074 del 26 de mayo de 2015 Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. La Dirección General se compromete a velar por la aplicación y cumplimiento adecuado de la política de tratamiento de datos personales y todas las que se deriven de ella, por parte de todos los funcionarios, contratistas y terceros de PROYECTAMOS SAS COLOMBIA. La Entidad reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo con la Ley de protección de datos personales 1581 de 2012, decreto 1377, Decreto 1074 o la que la adicione, modifique o derogue.

LINEAMIENTO DE ROLES Y RESPONSABILIDADES

Objetivo: Definir los Roles y Responsabilidades en Seguridad de la Información en PROYECTAMOS SAS

Todos los funcionarios, contratistas y terceros que ejercen funciones en PROYECTAMOS SAS y previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de la Entidad, son responsables del cumplimiento de las políticas, lineamientos procedimientos y normatividad vigente definida por la junta directiva de PROYECTAMOS SAS.

Todos los funcionarios, contratistas y terceros deben aplicar la Guía de Gestión Documental, y la Guía de organización de documentos electrónicos y archivamiento ya que de esta forma se garantiza la correcta gestión de la información de la entidad.

Todos los funcionarios, contratistas y terceros de la PROYECTAMOS SAS deben hacer buen uso de la información que se genera del desempeño de sus funciones laborales y/o actividades contractuales, y en ninguna circunstancia podrán divulgar información con categoría Pública Clasificada o Pública Reservada en espacios públicos o privados, mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre de PROYECTAMOS SAS. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.

Todos los activos de información de PROYECTAMOS SAS deben tener su propietario su custodio, y usuarios que deben estar debidamente identificados, esto de acuerdo con que sólo los Líderes de Proceso, son los que pueden desempeñar las veces de propietarios de activos de información, de acuerdo con esto son los responsables de tomar las medidas necesarias para la protección de la disponibilidad, confidencialidad e integridad de la información de los activos.

Tecnología de la información – Grupo de apoyo administrativo, Recursos Humanos, Contratación y Seguridad de la Información, deben definir la Matriz de Roles y Responsabilidades para cada activo de sistemas de información e infraestructura tecnológica, en la cual se deben incluir los roles y sus privilegios, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados. Si después de revisar la solicitud, se identifica que los privilegios solicitados no están definidos en la Matriz de Roles y Responsabilidades de los activos de información, se debe solicitar aprobación por parte del dueño del activo y se ejecutan por el Gestor de Accesos.

Todas las solicitudes de activación de usuarios deben tener fecha de finalización y cuando sean roles que no se encuentren en la Matriz serán considerados como Privilegios Temporales.

El Help Desk debe informar a través de los mecanismos de comunicación seleccionados, que el usuario fue creado y que fueron asignados los privilegios solicitados. Se debe capacitar a todos

los usuarios solicitantes de accesos a componentes tecnológicos sobre el uso y la responsabilidad que implica contar con esos privilegios. La Matriz de Roles y Responsabilidades debe ser actualizada periódicamente o cada vez que surja un cambio, de acuerdo a un requerimiento formal por parte del Líder del Proceso o responsable del Activos de Información. Todos los requerimientos deben ser solicitados formalmente a través del procedimiento establecido de creación de cuentas de usuarios.

LINEAMIENTOS PARA EL USO DE DISPOSITIVOS MÓVILES

Objetivo: Proteger la información almacenada en dispositivos móviles de PROYECTAMOS SAS.

Se debe llevar un registro y control de todos los dispositivos móviles que son propiedad de PROYECTAMOS SAS.

Todos los funcionarios, contratistas y terceros deben hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales y/o actividades contractuales.

El uso de dispositivos móviles fuera de las instalaciones sólo es autorizado a través del procedimiento formal de salida de dispositivos. Los dispositivos móviles que estén autorizados para salir y que contengan información sensible, se deben proteger mediante el uso de controles tecnológicos apropiados para ello, como cifrado de información, políticas de Restricción en la ejecución de aplicaciones, y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

Todos los dispositivos móviles que almacenen información de PROYECTAMOS SAS deben contar con un sistema de autenticación, como un patrón de movimiento, un código de desbloqueo o una clave.

Todos los dispositivos móviles que almacene información de PROYECTAMOS SAS deben tener instalado un software de antivirus.

Todos los dispositivos móviles que son propiedad de PROYECTAMOS SAS pueden estar monitoreados y ser sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

En caso de pérdida o robo de un dispositivo móvil que contenga información de PROYECTAMOS SAS, el funcionarios, contratistas o tercero que tiene a cargo del dispositivo móvil, debe avisar inmediatamente al personal del Help Desk o Tecnología de la información – Grupo de apoyo administrativo quienes cuentan con el procedimiento robo dispositivos móviles, que se debe realizar para tomar las acciones necesarias para la protección de la información.

Los funcionarios, contratistas y terceros responsables del dispositivo móvil deben hacer periódicamente copias de respaldo, en caso de los portátiles deben conectar el equipo mínimo una vez por semana a la red, e informar a Tecnología de la información – Grupo de apoyo administrativo con el fin de que se ejecute la copia de respaldo de la carpeta destinada para esta función.

Todos los funcionarios, contratistas y terceros son responsables de garantizar el buen uso de los dispositivos móviles, utilizarlos en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

Todos los dispositivos móviles propiedad de los funcionarios, contratistas y terceros, que requieran tener acceso a los servicios tecnológicos como el correo electrónico de PROYECTAMOS SAS, deben solicitar autorización mediante el procedimiento para ingreso seguro a los sistemas de información y estar debidamente identificados, con el fin de llevar el control y garantizar que se implementen las medidas de aseguramiento necesarias definidas por Tecnología de la información – Grupo de apoyo administrativo, de esta forma se puede garantizar la preservación de la disponibilidad, confidencialidad e integridad de la información de la PROYECTAMOS SAS.

La Tecnología de la información – Grupo de apoyo administrativo puede realizar borrado remoto de los datos en los dispositivos móviles de propiedad de la entidad; en caso de pérdida o cuando considere necesario de acuerdo con la **política de respaldo de información.**

SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo: Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información de PROYECTAMOS SAS, asegurando que los empleados y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que aspiran.

Incorporación de la Seguridad en la matriz de Cargos de la entidad

Deben ser incorporadas los roles y responsabilidades en seguridad de la información, en la matriz de responsabilidades de la Entidad.

Control y Política del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de PROYECTAMOS SAS.

Acuerdo de Confidencialidad

Todos los funcionarios, contratistas y terceros que ingresen a trabajar en PROYECTAMOS SAS, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Dentro del mismo acuerdo los funcionarios contratistas y terceros declaran conocer y aceptar que la PROYECTAMOS SAS se reserva el derecho de efectuar un monitoreo y control del uso que se realice servicios y activos informáticos de la entidad. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos de los funcionarios, contratistas y terceros.

Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación. Se deben aplicar los controles establecidos por la Entidad para otorgar el acceso a la información Pública Clasificada o Pública Reservada por parte del personal que resulte vinculado a la Entidad. El área de Recursos humanos y Contratos son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

Términos y condiciones Laborales

Todos los funcionarios, contratistas y terceros de PROYECTAMOS SAS deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar. Los términos y condiciones de trabajo establecidos en los contratos en PROYECTAMOS SAS deben establecer la responsabilidad del funcionario por la seguridad de los activos de información y aclarar que va más allá de la finalización de la relación laboral. Esto se hace extensivo a aquellos contratistas y terceros que tengan acceso a la información en la Entidad por medio de los contratos respectivos. Todos los funcionarios, contratistas y terceros, durante el proceso de vinculación a PROYECTAMOS SAS, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

Entrenamiento, concientización y capacitación

Todos los funcionarios, contratistas y terceros de PROYECTAMOS SAS deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

Formación y Capacitación en Materia de Seguridad de la Información

Todos los funcionarios, contratistas y terceros cuando sea el caso, que trabajen para PROYECTAMOS SAS deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de seguridad y privacidad de la Información. Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Entidad para el desempeño de sus funciones laborales y/o actividades contractuales.

Procesos disciplinarios

Los funcionarios, contratistas y terceros de PROYECTAMOS SAS deben cooperar en los esfuerzos por proteger la información y son responsables de actualizarse en la materia, así como consultar con el oficial de seguridad y privacidad de la información de la Entidad en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera del proceso disciplinario correspondiente a violaciones de la política y del manual de lineamientos de seguridad y privacidad de la información. Todos los incidentes de seguridad de la información presentados en PROYECTAMOS SAS deben tener el tratamiento adecuado y establecido en el

procedimiento de gestión de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables. Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes. En lo pertinente a la violación de las políticas de seguridad de la información de la Entidad, a los funcionarios, contratistas y terceros, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

LINEAMIENTOS PARA EL USO DE CORREO ELECTRÓNICO

Objetivo: Definir las directrices generales del buen uso del correo electrónico en PROYECTAMOS SAS.

Usos aceptables del servicio

- Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en PROYECTAMOS SAS y no se debe utilizar para otros fines.
- La información clasificada como Pública Reservada o Pública clasificada debe cifrarse para ser transmitida por correo electrónico, y contar con la autorización para su envió.
- Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de PROYECTAMOS SAS
- Todos los funcionarios, contratistas y terceros que son autorizados para acceder a la red de datos y los servicios de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.
- Todos los funcionarios, contratistas y terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información de PROYECTAMOS SAS.
- El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con PROYECTAMOS SAS. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de PROYECTAMOS SAS y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.
- Cuando un Proceso, Oficina, Grupo o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones de PROYECTAMOS SAS o el medio formal autorizado para realizar esta actividad.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por PROYECTAMOS SAS y deberán conservar en todos los casos el mensaje legal de la entidad. El único servicio de correo electrónico controlado en la entidad es el asignado directamente por Tecnología de la información – Grupo de apoyo administrativo, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de Malware o código malicioso.
- El servicio de correo electrónico debe contar con respaldo de información (Back up) que deben ser aplicados de manera periódica y segura.

- Se debe incluir en la copia de respaldo la Información de los registros de auditoría que generan los buzones de correo.
- Para acceder al correo electrónico desde canales externos a los de PROYECTAMOS SAS, se debe garantizar que la información viaja cifrada.
- Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Pública Reservada o Pública Clasificada), de acuerdo a la Clasificación y Etiquetado de la Información establecida en la entidad.
- El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por Tecnología de la información – Grupo de apoyo administrativo.
- El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos sospechosos o de dudosa procedencia o con virus a Tecnología de la información – Grupo de apoyo administrativo, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y esté seguro que este no es de tipo SPAM, así Tecnología de la información – Grupo de apoyo administrativo hace el análisis para evaluar el origen y así tomar las medidas pertinentes.
- Cuando un usuario se retire de PROYECTAMOS SAS, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio del correo de la entidad, debe abstenerse de continuar utilizándolas y se debe verificar que su cuenta y acceso a los servicios sean cancelados.
- Los mensajes y la información contenida en los buzones de correo son de propiedad de PROYECTAMOS SAS.
- Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.
- La información almacenada en el buzón de correo, es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.
- Las cuentas institucionales (Ejemplo: Comunicaciones, atención al ciudadano, Soporte, control interno etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.
- Todas las comunicaciones de mercadeo realizadas por correo electrónico, dirigidas a usuarios encontrados en la base de datos de contactos en PROYECTAMOS SAS, deben incluir

instrucciones de cómo los destinatarios pueden solicitar ser removidos rápidamente de la base de datos de contactos y detener comunicaciones, correos o mensajes posteriores.

- Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto.

- En los casos en que el usuario desconfíe del remitente de un correo electrónico debe remitir la consulta al Help Desk.

- Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), Tecnología de la información – Grupo de apoyo administrativo actuará según sea el caso. Tecnología de la información – Grupo de apoyo administrativo se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos.

- Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.

- Ningún usuario debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

- El usuario no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a Tecnología de la información – Grupo de apoyo administrativo, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de PROYECTAMOS SAS.

- Toda cuenta de correo es de propiedad de PROYECTAMOS SAS y los buzones que no sean utilizados en un tiempo superior a cuarenta y cinco (45) días se inactivan por Tecnología de la información – Grupo de apoyo administrativo. Todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar mensajes es de 25 MB (incluyendo la suma de todos los adjuntos).

- Todos los mensajes de correo electrónico deben contener el nombre y apellidos del remitente, su cargo, grupo de trabajo al que pertenece y número telefónico.

- En todos los mensajes de correo electrónico salientes, debe agregarse un pie de página avalado por la Dirección General que indique que el mensaje puede contener información Pública clasificada, que es para el uso de los destinatarios nombrados, que ha sido registrado para propósitos de archivo.

- Todos los usuarios de correo en PROYECTAMOS SAS deben analizar todos los mensajes de

correo electrónico entrantes, en busca de software malicioso y contenido ajeno a la entidad y no deben abrir archivos adjuntos a los correos electrónicos, a menos que esté seguro de que ya han sido analizados por el software de detección, eliminación y reparación de código malicioso aprobado.

Usos no aceptables del servicio

- Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.
- Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus o malware
- Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.
- Envió de mensajes que contengan amenazas o mensajes violentos.
- Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.
- Divulgación no autorizada de información propiedad de PROYECTAMOS SAS. Los usuarios no deben reenviar correo electrónico a direcciones externas a PROYECTAMOS SAS, a menos que exista autorización previa del propietario de la información o que la información sea pública por naturaleza.
- Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización. Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.
- Los usuarios del servicio del correo electrónico no pueden modificar, falsificar o eliminar cualquier información contenida en los mensajes, incluyendo el cuerpo y los encabezados.
- Enviar correos masivos, con excepción de funcionarios con nivel de director o superior, quienes sean previamente autorizados por éstos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.
- Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

LINEAMIENTOS PARA EL USO DE INTERNET

Objetivo: Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información de PROYECTAMOS SAS.

Usos aceptables del servicio

- La solicitud del servicio de internet se debe hacer mediante el procedimiento para ingreso seguro a los sistemas de información.
- Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en PROYECTAMOS SAS y no debe utilizarse para ningún otro fin.
- Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de PROYECTAMOS SAS.
- Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.
- El navegador autorizado para el uso de Internet en la red de PROYECTAMOS SAS es el instalado por Tecnología de la información – Grupo de apoyo administrativo, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.
- No se permite la conexión de módems externos o internos en la red de PROYECTAMOS SAS, previa solicitud autorizada por Tecnología de la información – Grupo de apoyo administrativo.
- El acceso a internet por cada usuario depende del rol que desempeñe en PROYECTAMOS SAS y para los cuales esté formal y expresamente autorizado. Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.
- PROYECTAMOS SAS se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.
- Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o malintencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.
- Los funcionarios, contratistas y terceros de PROYECTAMOS SAS no deben asumir en nombre de la entidad, posiciones personales en encuestas de opinión, foros u otros medios similares.
- Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de PROYECTAMOS SAS.

- Todos los usuarios invitados que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

Usos no aceptables del servicio

- Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.
- Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.
- Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.
- No se permite el acceso a páginas con contenido restringido como pornografía, anonimizados, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos de PROYECTAMOS SAS y las emitidas por los entes de control.
- No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

Objetivo: Definir los lineamientos generales para el uso del servicio de mensajería instantánea por parte de los usuarios en PROYECTAMOS SAS.

Mensajería instantánea

- WhatsApp es la única herramienta de mensajería instantánea permitida en PROYECTAMOS SAS.

No se debe utilizar la mensajería instantánea en conversaciones confidenciales o para transmitir o recibir información crítica o sensible. Los usuarios del servicio de mensajería instantánea no pueden utilizar comentarios obscenos, despectivos u ofensivos en contra de cualquier persona o entidad

LINEAMIENTOS DE USO DE REDES SOCIALES

Objetivo: Definir los lineamientos generales para el uso del servicio de Redes sociales por parte de los usuarios autorizados en PROYECTAMOS SAS.

Usos aceptables del servicio

- Todos los usuarios autorizados por la dirección para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de PROYECTAMOS SAS.
- El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con PROYECTAMOS SAS.
- Todas las comunicaciones establecidas mediante este servicio deben ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control que lo requiera.
- Es permitido el uso de redes sociales utilizando videoconferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.
- No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso
- No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calúmniate a través del servicio de Redes Sociales
- No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet de PROYECTAMOS SAS, o aprovechar el acceso a Redes Sociales para fines ilegales.
- No se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.
- Todos los funcionarios, contratistas y terceros de PROYECTAMOS SAS, deben seguir los procedimientos y planes de comunicaciones interna y externa.
- Tecnología de la información – Grupo de apoyo administrativo, será el encargado de brindar asesoría en diferentes herramientas o plataformas de apoyo a la gestión de las redes sociales en PROYECTAMOS SAS que pueden ser usadas, previo acuerdo con el Sub Proceso de Comunicaciones
- El acceso a las plataformas para la gestión de las redes sociales se debe controlar mediante mecanismos de doble autenticación, lo cuales deben estar a cargo del Comunity Manager.
- Cumplir con la circular No 001 2019 de la presidencia de la república “Manejo y Uso de redes sociales”

LINEAMIENTOS PARA EL USO DE RECURSOS TECNOLÓGICOS

Objetivo: Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos de PROYECTAMOS SAS.

PROYECTAMOS SAS asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los funcionarios, contratistas y terceros de ser necesario.

Usos aceptables del servicio

- Antes que cualquier sistema operativo sea puesto en operación en PROYECTAMOS SAS, Tecnología de la información – Grupo de apoyo administrativo debe aplicar las líneas base de seguridad requerida para el cumplimiento del modelo de privacidad y seguridad de la información.
- Sólo el personal designado por Tecnología de la información – Grupo de apoyo administrativo está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnología de PROYECTAMOS SAS.
- Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla de la entidad.
- Estos cambios únicamente deben ser realizados por Tecnología de la información – Grupo de apoyo administrativo.
- Tecnología de la información – Grupo de apoyo administrativo es el responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en PROYECTAMOS SAS para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- Sólo el personal autorizado por Tecnología de la información – Grupo de apoyo administrativo podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de PROYECTAMOS SAS; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la entidad.
- Se debe garantizar que todas las licencias de software base y software de aplicación cumplen con las arquitecturas tecnológicas y de aplicaciones de PROYECTAMOS SAS, y que están legalizadas mediante una adquisición, antes de proceder a su instalación y despliegue en la infraestructura de TI de la Entidad.
- Los funcionarios, contratistas y terceros son responsables de hacer buen uso de los recursos tecnológicos de PROYECTAMOS SAS y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o malintencionadas que atenten contra otros funcionarios, contratistas o terceros, legislación vigente y políticas y lineamientos de

seguridad de la información establecidas por PROYECTAMOS SAS.

- Todo activo informático propiedad de PROYECTAMOS SAS, asignado a un servidor público o tercero de PROYECTAMOS SAS, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye: Activos de software, Activos físicos, Activos de información, Activos intangibles ejemplo: los documentos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

- Se deben realizar revisiones cada vez que se complete un ciclo de gestión de seguridad de la información o realizar evaluaciones de vulnerabilidades sobre los sistemas operativos de producción, para proteger la información asociada con la interconexión de los sistemas de información en PROYECTAMOS SAS.

- Todos los funcionarios, contratistas y terceros son responsables de informar cualquier tipo de incidencia de ciberseguridad como virus, suplantación de identidad, Spam, ataques informáticos o si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de PROYECTAMOS SAS, para que de esta forma Tecnología de la información – Grupo de apoyo administrativo realice el ajuste de permisos requerido.

LINEAMIENTOS RELACIONADOS CON LA CLASIFICACIÓN, CONTROL Y PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN

Objetivo: Asegurar que la información de PROYECTAMOS SAS es clasificada, con el fin de que sea tratada y protegida adecuadamente.

Identificación, clasificación e inventario de activos de información

- La información de PROYECTAMOS SAS, así como los activos donde ésta se almacena y se procesa deben ser inventariados, asignados a un responsable y clasificados de acuerdo con los requerimientos y los criterios que se definan para tal fin. Se debe establecer un Procedimiento De Identificación Y Clasificación De Activos que permita claramente identificar el nivel de seguridad requerido por cada activo de información, de acuerdo con las necesidades de la Entidad.

- Los responsables del levantamiento de los activos de información se encuentran en cabeza de las personas delegadas por los Procesos y/o Subprocesos de Seguridad y Privacidad de la Información, Gestión Documental, Direccionamiento Estratégico y Tecnología de la información – Grupo de apoyo administrativo, quienes se encargan de liderar la ejecución y mantenimiento del Inventario de Activos

Periodicidad de la Identificación, clasificación e inventario de activos de información.

Los activos de información de PROYECTAMOS SAS deberán actualizarse, y/o modificarse por lo menos una vez al año o cuando se haga necesario la modificación o inclusión de los mismos.

Esquema de Clasificación de la Información

El subsistema de Seguridad y Privacidad de la información, Tecnología de la información – Grupo de apoyo administrativo y el Proceso de Gestión Documental son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo con la clasificación establecida por la entidad y el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:

• Nivel de clasificación.

• Acceso a la información sólo de personal autorizado.

• Llevar un registro formal de acceso a la información.

• Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

El nivel de clasificación de la información debe revisarse cada vez que se realice un ciclo de gestión y cuando se presenten cambios en la información o en la estructura que puedan afectarla.

Etiquetado y manejo de Información

- Se debe llevar permanentemente para cada activo, información detallada sobre su valoración en confidencialidad, integridad, disponibilidad y auditabilidad, así como los procesos de tratamiento, marcación e información relevante para su gestión.
- Cada una de los procesos y subprocesos que administran o utilizan activos de información de la UAE
- PROYECTAMOS SAS gestionará que estén claramente identificados y deberá mantener y elaborar un inventario actualizado.
- Todos los funcionarios, contratistas y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.
- La Dirección, los Asesores o Líderes de Procesos/Subprocesos deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.
- Todos los funcionarios, contratistas y terceros cuando sea el caso de PROYECTAMOS SAS son responsables de la organización, conservación, uso y manejo de los documentos; de acuerdo con las políticas internas de la entidad y/o el archivo general de la nación.
- Todas las dependencias de PROYECTAMOS SAS deben transferir a gestión documental la documentación de forma ordenada y organizada, de acuerdo con los tiempos de retención establecidos en la Tabla de Retención Documental y el Manual de Gestión Documental, acompañado del formato único de inventario documental FUID y en medio magnético.
- El área de gestión documental de PROYECTAMOS SAS recibe las transferencias documentales de acuerdo con el cronograma anual de transferencia Documentales.
- El área de gestión documental de PROYECTAMOS SAS debe custodiar los documentos de acuerdo con lo especificado en las tablas de Retención Documental y procedimientos establecidos.
- La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en forma digital y electrónica debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.
- Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por PROYECTAMOS SAS.
- El etiquetado de información debe incluir la información física y electrónica. Las etiquetas de la información se deben identificar y reconocer fácilmente.

- Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.
- Al imprimir documentos de carácter Pública Clasificada o Pública Reservada, deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información Pública Clasificada o Pública Reservada.

Usos no aceptables

- Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias, de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.
- Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.
- Divulgación no autorizada de los expedientes, documentos, información o archivos
- Realizar actividades tales como borrar, modificar, alterar o eliminar información de PROYECTAMOS SAS de manera malintencionada tanto en soporte físico, electrónico como también la información que se encuentra en el sistema de gestión documental.

Investigación de la información que reside en los diferentes medios tecnológicos que posee PROYECTAMOS SAS

La información física, electrónica y/o digital o que se encuentre en el sistema de gestión documental podrá ser investigada por mandato de la Dirección General y por Control Interno o quien haga sus veces, mediante solicitud escrita y bajo la premisa de cumplimiento de la ley.

Respaldo de la información

PROYECTAMOS SAS con el fin de proteger la información ha destinado las siguientes unidades de red:

• Unidad (G:) (Google Drive File Stream): En esta unidad todo funcionario o contratista de la entidad debe salvaguardar la información de uso diario y está bajo la responsabilidad es del usuario.

• Unidad (J:): Esta es la unidad ubicada en el servidor y está destinada a salvaguardar los documentos finales, es la unidad del equipo de trabajo y está bajo la responsabilidad es del líder del proceso o sub proceso.

Tecnología de la información – Grupo de apoyo administrativo, es el responsable de realizar las copias de seguridad de la Unidad J acorde a los Lineamientos de Backup de la Entidad, para la unidad G: la entidad cuenta con el servicio de Backupify.

Clasificación de la información

Toda información de PROYECTAMOS SAS mientras no haya sido clasificada, debe ser tratada como Pública Clasificada. Es potestad y obligación de quien genera información clasificarla de acuerdo con los criterios que se establezcan y esta clasificación mantenerla actualizada.

Propiedad de la información

PROYECTAMOS SAS es propietaria de toda la información que generan, procesan e intercambian y constituye parte de su activo.

LINEAMIENTOS PARA LA GESTIÓN DE MEDIOS DE ALMACENAMIENTO

Objetivo: Proteger la información de PROYECTAMOS SAS velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Gestión y Disposición de medios removibles

- Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, tarjetas de memoria portátiles "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de PROYECTAMOS SAS y uso hasta finalización de su contrato o cese de actividades.

- Toda la información clasificada como Pública Clasificada o Pública Reservada que sea almacenada en medios removibles y que se requiera de protección especial, debe cumplir con las directrices de seguridad emitidas por el Tecnología de la información – Grupo de apoyo administrativo, específicamente aquellas referentes al empleo de técnicas de cifrado.

- Se debe llevar el registro de todos los medios removibles de PROYECTAMOS SAS y mantenerlo actualizado. Todos los medios removibles deben ser almacenados de manera segura.

- Tecnología de la información – Grupo de apoyo administrativo puede restringir qué medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de PROYECTAMOS SAS o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

- Los medios de almacenamiento removibles que se conecten a la red de datos de PROYECTAMOS SAS o que se encuentren bajo su custodia, están sujetos a monitoreo por parte de Tecnología de la información – Grupo de apoyo administrativo.

- Todos los retiros de medios de almacenamiento de las instalaciones de PROYECTAMOS SAS, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo con el mapa de procesos de PROYECTAMOS SAS, a través del formato orden de salida de elementos.

- Todos los medios de almacenamiento removibles propiedad de PROYECTAMOS SAS, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

- Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc., con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

- Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por PROYECTAMOS SAS para su uso dentro de la red corporativa, deben contar con su respectivo soporte

Borrado seguro

- Los medios de almacenamiento que contienen información sensible (discos compactos, discos duros, tarjetas de memoria portátiles, documentos, etc.) deben ser formateados por Tecnología de la información – Grupo de apoyo administrativo y posteriormente sometidos al comité de altas y bajas para indicar su disposición final.
- Todos los medios de almacenamiento que contengan información de PROYECTAMOS SAS y que salgan de la Entidad y que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por PROYECTAMOS SAS, el cual garantiza que la información no sea recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, etc.).
- Los medios de almacenamiento que contengan información de PROYECTAMOS SAS y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por PROYECTAMOS SAS, el cual garantiza que la información no sea recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por desgaste o falla son retirados o dados de baja).
- Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información de PROYECTAMOS SAS.

Transferencia de medios físicos

Toda la información clasificada como Pública Clasificada o Pública Reservada que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones de PROYECTAMOS SAS, debe cumplir con las disposiciones de seguridad indicadas por Tecnología de la información – Grupo de apoyo administrativo, específicamente aquellas referentes al empleo de técnicas de cifrado.

El transporte de los medios físicos debe cumplir con lo establecido en el Acuerdo 008 del 2014, además debe hacerse mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evitar una afectación a la integridad y disponibilidad.

Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.

LINEAMIENTOS RELACIONADOS CON EL CONTROL DE ACCESO

Objetivo: Definir las directrices generales para un acceso controlado a la información de PROYECTAMOS SAS.

Control de Acceso a Redes y Servicios en Red

- PROYECTAMOS SAS suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales y/o actividades contractuales.
- Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.
- Toda actividad que requiera acceder a los servidores, equipos o a las redes de PROYECTAMOS SAS, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización de Tecnología de la información – Grupo de apoyo administrativo.
- Tecnología de la información – Grupo de apoyo administrativo de PROYECTAMOS SAS evaluarán, de acuerdo con la disponibilidad de recursos y a los aspectos de seguridad, la pertinencia y establecerán las acciones de mitigación de riesgos para atender la solicitud de autorización para que usuarios externos puedan usar y/o acceder a los elementos de TI. El que autorice el acceso será responsable por garantizar que se implementen los mecanismos legales o de control de dichas acciones, y de esta manera cubrir adecuadamente las consecuencias del accionar del usuario externo autorizado.
- La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento para ingreso seguro a los sistemas de información
- Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.
- Las cuentas de usuarios administradores deben tener justificación y deben ser controladas.

Gestión de Acceso a Usuarios

- Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.
- Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire
- Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.
- El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 30 días.

- Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por elHelp Desk.
- Se debe mantener como mínimo un registro de las 3 últimas contraseñas utilizadas por el usuario, y evitar la reutilización de estas.
- Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.
- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional
- Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo, appliance, impresoras, routers, switch, herramientas de seguridad, etc.).
- No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, lideres u otras personas que lo soliciten.
- Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.
- Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
- Reportar a el HELPDESK y al Oficial de Seguridad y Privacidad de la información sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
- Reportar a el HELPDESK y al Oficial de Seguridad y Privacidad de la información sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.
- Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada DOS (2) meses.
- Los permisos de acceso a los recursos informáticos y servicios de la red de datos deben ser solicitados y aprobados por los responsables de los sistemas de información.
- El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por Tecnología de la información – Grupo de apoyo administrativo.

Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información de PROYECTAMOS SAS, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos y/o subprocesos.

Retiro de los derechos de acceso

Cada uno de los líderes y/o supervisores de los procesos de la Entidad son los responsables de comunicar a la Oficina de Recursos Humanos y/o Contratación, el cambio de cargo o funciones o actividades, vacaciones, suspensión o la terminación contractual de los Colaboradores pertenecientes al proceso. La Oficina de Recursos Humanos y/o Contratación son las encargadas de comunicar a Tecnología de la información – Grupo de apoyo administrativo, almacén y a Gestión Documental sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de PROYECTAMOS SAS.

Perímetro de Seguridad Física

- Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los funcionarios, contratistas y terceros autorizados evitar que las puertas se dejen abiertas.
- Las instalaciones en las cuales se realice o contenga equipos de procesamiento de datos y/o información crítica o sensible de PROYECTAMOS SAS deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido.
- Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de PROYECTAMOS SAS.
- Todos los funcionarios, contratistas y terceros cuando sea el caso, sin excepción deben portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de PROYECTAMOS SAS.
- Está prohibido prestar el carnet de identificación y tarjeta de acceso, se considera como suplantación de identidad por parte de la persona que lo usa sin ser la persona autorizada.
- Los visitantes deben permanecer acompañados de un funcionario o colaborador de PROYECTAMOS SAS, cuando se encuentren en las oficinas o áreas donde se maneje información.
- Es responsabilidad de todos los funcionarios, contratistas y terceros de PROYECTAMOS SAS borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones
- Los visitantes que requieran permanecer en las oficinas de PROYECTAMOS SAS por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.
- El horario de prestación de servicios en las instalaciones de PROYECTAMOS SAS es de lunes a viernes desde las 6:00 AM hasta las 6:00 PM. En horarios distintos se requerirá de la autorización del director, Asesor o Líder de Proceso/Subproceso.
- El horario autorizado para recibir visitantes en las instalaciones de PROYECTAMOS SAS es de lunes a viernes desde las 8:00 AM hasta 5:00 PM. En horarios distintos se requerirá de la autorización del director, Asesor o Líder de Proceso/Subproceso.
- Los dispositivos removibles, así como toda información Pública Clasificada y/o Pública Reservada de PROYECTAMOS SAS, independientemente del medio en que se encuentre, deben

permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales el funcionario, Colaborador o Tercero responsable no se encuentre en su sitio de trabajo.

- Las instalaciones de PROYECTAMOS SAS deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de los funcionarios, contratistas, terceros y visitantes.

Controles de Acceso Físico

- Las áreas seguras, dentro de las cuales se encuentran el Cuarto técnico, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información, deben ubicarse en lugares a los cuales se pueda controlar y evitar cualquier acceso no autorizado y no deben tener ningún tipo de señalamiento.
- Los derechos de acceso a las áreas seguras de PROYECTAMOS SAS deben actualizarse cada vez que ocurra una novedad del personal que tiene derecho de acceso a estas instalaciones, de manera que se evite el acceso de personal no autorizado.
- El acceso físico y lógico a la información crítica o sensible y a las áreas seguras de PROYECTAMOS SAS, debe ser controlado y limitado exclusivamente a las personas autorizadas.
- Debe mantenerse un registro protegido que permita auditar todos los accesos a las áreas seguras de PROYECTAMOS SAS.
- En las áreas seguras, en ninguna circunstancia se puede fumar, comer o beber.
- Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia que no represente riesgo para las áreas seguras de PROYECTAMOS SAS.
- Las condiciones ambientales deben ser monitoreadas para verificar desviaciones que afecten de manera adversa el funcionamiento de los equipos de procesamiento en PROYECTAMOS SAS.
- Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un funcionario o colaborador del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

Ubicación y Protección de los equipos.

- La información crítica o sensible para PROYECTAMOS SAS debe permanecer distribuida en áreas seguras y protegidas físicamente contra acceso no autorizado, daño o indisponibilidad.
- La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados

- Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.
- Aquellas áreas desocupadas aledañas a las áreas seguras de PROYECTAMOS SAS deben ser físicamente bloqueadas y periódicamente inspeccionadas.

Seguridad de los equipos fuera de las instalaciones

- Los equipos de procesamiento de datos (estaciones de trabajo, portátiles, etc.) utilizados para realizar trabajos fuera de la sede principal y oficinas seccionales de PROYECTAMOS SAS, deben cumplir con las directrices establecidas.
- Los equipos portátiles que contengan información clasificada como Pública Clasificada o Pública Reservada, deben ser controlados mediante el cifrado de la información almacenada en sus discos duros, utilizando la herramienta definida por Tecnología de la información – Grupo de apoyo administrativo.
- Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.
- En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al Proceso de Gestión Administrativa y a Tecnología de la información – Grupo de apoyo administrativo y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.
- Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones de PROYECTAMOS SAS.
- Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de PROYECTAMOS SAS.

Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de PROYECTAMOS SAS sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de PROYECTAMOS SAS.

LINEAMIENTOS DE ESCRITORIO Y PANTALLA LIMPIOS

Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla libre de información sin control, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de PROYECTAMOS SAS.

- Todo el personal de PROYECTAMOS SAS debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.
- Todo el personal de PROYECTAMOS SAS debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.
- Todos los personales al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.
- En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, el personal debe dejar la información Pública Clasificada y/o Pública Reservada protegida bajo llave.

LINEAMIENTOS PARA LA GESTIÓN DE CAMBIOS

Objetivo: Asegurar que los cambios a nivel de infraestructura, software base (SO), aplicaciones y sistemas de información realizados en PROYECTAMOS SAS se realicen de forma controlada.

- Se deben establecer procedimientos para el control de cambios ejecutados en la entidad.
- Toda solicitud de cambio en los servicios de procesamiento de información de PROYECTAMOS SAS, se debe realizar siguiendo el Procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.
- Se debe llevar una trazabilidad del control de cambios solicitados.
- En el procedimiento de gestión de cambios se debe especificar los canales autorizados para la recepción de solicitudes de cambios, como el Help Desk, correo electrónico o un oficio dirigido al Líder de Tecnología de la información – Grupo de apoyo administrativo.
- Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.
- Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.
- Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los funcionarios, contratistas y terceros que por sus funciones tienen relación con el sistema de información.
- Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.
- Los cambios realizados sobre sistemas de información deben ser probados en un ambiente de pruebas para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente y así poder ser puesto en el ambiente de producción.
- Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida en de PROYECTAMOS SAS.

Requerimientos de seguridad que deben manejarse en los sistemas de información

- Se debe realizar un adecuado análisis e implementación de los requerimientos de seguridad del software, ya sea interno o adquirido, que incluya garantías de validación de usuarios, datos de entrada y salida; y del procesamiento de los mismos, de acuerdo con la clasificación de los activos a tratar en el sistema.
- Los propietarios de la información deben considerar los requerimientos de seguridad necesarios para mantener la integridad y confidencialidad de su información por ellos administrada. Es responsabilidad del propietario de la información la incorporación de los controles relevantes en el nuevo sistema. Este lineamiento debe ser expandida a sistemas que reciban modificaciones significativas, no solo para nuevos desarrollos.

Programas especiales para acceder, crear o modificar datos en un sistema

Se deben diseñar procedimientos controlados (programas o porciones de programa), las cuales deben ser los únicos que se puedan seguir para poder crear, acceder y modificar datos en los sistemas. Se debe evitar el uso de instrucciones primarias para realizar las operaciones sobre datos.

Autorización para modificar información

Únicamente personas autorizadas pueden modificar la información sensible y crítica en PROYECTAMOS SAS. La confirmación de la autorización puede realizarse a través de firmas digitales, certificados digitales.

Autenticación, trazabilidad y auditoría de información modificada

Los sistemas deben disponer de funcionalidad que permitan autenticar todos los mensajes y actualizaciones a los registros de las bases de datos de información, así como preservar la integridad de los registros en PROYECTAMOS SAS. Si son ingresadas transacciones no autorizadas a los registros, entonces éstos pasan a ser de valor cuestionable. Los sistemas deben tener la opción de configurar auditorías y tener opciones de poder determinar la trazabilidad de la información cuando fue creada o modificada.

Copias de los programas que generen o verifiquen firmas digitales

Se deben mantener copias confiables de los programas de computador que se utilicen para generar o verificar firmas digitales, o para cifrar o descifrar archivos, con el fin de tener la posibilidad de que un usuario pueda probar que firmó un archivo en casos judiciales, procedimientos de arbitramento o procesos de mediación y para recuperar un archivo previamente encriptado.

Almacenamiento de programas fuentes

Se debe mantener un sistema de almacenamiento seguro y centralizado de programas fuente.

Autenticación fuerte en sistemas y servidores de PROYECTAMOS SAS

Los usuarios de PROYECTAMOS SAS involucrados en comunicaciones con terceros, deben utilizar esquemas de autenticación fuerte que permitan a un tercero verificar que está accediendo un sistema genuino en la Entidad.

Cifrado de información que se maneje en sistemas o servidores de PROYECTAMOS SAS

Para el cifrado se deben utilizar algoritmos fuertes y probados. Los sistemas de cifrado utilizados para las actividades regulares en PROYECTAMOS SAS deben incluir funciones de recuperación de llaves. Las llaves de cifrado deben ser protegidas con las medidas de seguridad más exigentes. Esto requiere que las llaves de cifrado sean a su vez cifradas y se almacenan en archivos u otras locaciones donde no puedan ser accedidas por personas no autorizadas.

LINEAMIENTOS PARA LA SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

Objetivo: Reducir riesgos asociados a modificaciones, alteraciones, cambios o accesos no autorizados en sistemas en producción de PROYECTAMOS SAS.

- PROYECTAMOS SAS debe establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información de la Entidad.
- Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo con el inventario y clasificación de activos de información.
- El ambiente de desarrollo se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo. Por último, el ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la entidad.
- En la Entidad se debe seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo, pruebas y producción), donde se establecen las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo con el inventario y clasificación de activos de información.
- No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
- En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción, sin antes haber pasado por un proceso de ofuscamiento.
- Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento de este.
- Se deben utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
- Las interfaces de los sistemas deben ser identificadas claramente para poder determinar a qué instancia se está realizando la conexión.
- Los ambientes deben estar claramente identificados, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada uno.
- Los cambios a sistemas en producción que involucren aspectos funcionales deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información.
- Se debe establecer una guía para el desarrollo seguro de software en PROYECTAMOS SAS.

LINEAMIENTOS PARA PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en PROYECTAMOS SAS.

- Debe instalarse software de detección, eliminación y reparación de código malicioso a nivel de los Firewalls, servidores y en las estaciones de trabajo de los usuarios y debe certificarse que todo el software, archivos o ejecutables, se encuentran libres de virus antes de ser instalado en la infraestructura de PROYECTAMOS SAS o enviados a una entidad externa
- Se debe restringir la ejecución de aplicaciones y mantener activo y actualizado el antivirus, en todas las estaciones de trabajo y servidores de PROYECTAMOS SAS.
- Todos los sistemas sin las actualizaciones de seguridad requeridas o los sistemas infectados con cualquier tipo de malware deben ser desconectados de las redes en PROYECTAMOS SAS.
- Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.
- Todos los funcionarios, contratistas y terceros que sospechen de una infección por código malicioso deben apagar inmediatamente el computador involucrado, desconectarlo de cualquier red, reportarlo a través del Help Desk y evitar hacer intentos de eliminarlo. Una infección por código malicioso de computador solo debe ser tratada por el responsable asignado en PROYECTAMOS SAS.
- PROYECTAMOS SAS cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por Tecnología de la información – Grupo de apoyo administrativo.
- El antivirus adquirido por PROYECTAMOS SAS, sólo debe ser instalados por los responsables de Tecnología de la información – Grupo de apoyo administrativo.
- Los equipos de terceros que son autorizados para conectarse a la red de datos de PROYECTAMOS SAS deben tener antivirus y contar con las medidas de seguridad apropiadas.
- Todos los equipos conectados la red de PROYECTAMOS SAS pueden ser monitoreados y supervisados por la Oficina de Tecnologías de la Información y las Comunicaciones
- Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.
- Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de Tecnología de la información – Grupo de apoyo administrativo.
- La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios

de almacenamiento removibles, contenido de correo electrónico, etc.

- Se deben hacer campañas de sensibilización a todos los funcionarios, contratistas y terceros de ser el caso, con el fin de generar una cultura de seguridad de la información.
- No deben transferir (subir y bajar) software desde y hacia sistemas que se encuentran por fuera o en PROYECTAMOS SAS.
- No deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos a menos que el software haya sido examinado en busca de código malicioso y que haya sido aprobado por Tecnología de la información – Grupo de apoyo administrativo de PROYECTAMOS SAS.
- Es responsabilidad de los funcionarios, contratistas y terceros que utilicen medios de almacenamiento como USB, CD-ROM, Discos Externos etc., provistos por entidades externas analizar con sistemas antivirus antes de ser utilizados en los sistemas de PROYECTAMOS SAS.
- Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, sin la previa autorización de Tecnología de la información – Grupo de apoyo administrativo.
- Los funcionarios, contratistas y terceros de PROYECTAMOS SAS pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los funcionarios, contratistas y terceros cuando sea necesario siempre podrán consultar a Tecnología de la información – Grupo de apoyo administrativo sobre el tratamiento que debe darse en caso de sospecha de malware.
- Los funcionarios, contratistas y terceros no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales y/o actividades contractuales.
- Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por PROYECTAMOS SAS, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta del Help Desk.
- El único servicio de antivirus autorizado en la entidad es el asignado directamente por Tecnología de la información – Grupo de apoyo administrativo el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por Tecnología de la información – Grupo de apoyo administrativo, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

- Tecnología de la información – Grupo de apoyo administrativo es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red de PROYECTAMOS SAS.
- Tecnología de la información – Grupo de apoyo administrativo se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o transporten y almacenen en cualquier medio, en busca de virus o código malicioso.
- Tecnología de la información – Grupo de apoyo administrativo se reserva el derecho de filtrar los contenidos que se transmitan en la red de PROYECTAMOS SAS, con el fin de evitar amenazas de virus.
- Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, el correo será eliminado.

Objetivo: Proporcionar medios de respaldo de información adecuados en PROYECTAMOS SAS para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla

- Tecnología de la información – Grupo de apoyo administrativo, debe realizar periódicamente una validación con los propietarios de la información para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar, esto debe quedar documentado

en los acuerdos de nivel de servicio.

- Tecnología de la información – Grupo de apoyo administrativo y el Oficial de SIP, junto a los propietarios de la información deben determinar los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI.
- Tecnología de la información – Grupo de apoyo administrativo debe disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de PROYECTAMOS SAS.
- Se debe definir y documentar un esquema de respaldo de la información.
- El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.
- Se debe tener en cuenta los lineamientos de la ley 594 de 2000 o cualquiera que la modifique, adicione o derogue.
- Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.
- Se deben definir procedimientos para el backup de la información, que incluyan los siguientes parámetros:
- Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Definir en el procedimiento como sería el reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo a lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.
- Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.
- Se deben retener por lo menos por tres periodos los activos de información de PROYECTAMOS SAS.
- Para realizar las copias de respaldo en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado por la Entidad a los que se encuentre sujeta.
- Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

- Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.
- La entidad debe contar con un sistema que le permita:
- Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.
- Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.
- Realizar una copia de respaldo de los Servidores de Base de Datos, servidores Web, Sistemas de Información misionales, Aplicaciones, Desarrollo y dispositivos de red.
- Las copias de respaldo se deben realizar en horario no hábil, lo cual será verificado a través de Procesos Automáticos.
- Los medios de almacenamiento de backup que contienen información crítica, deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.
- El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.
- Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.
- Tecnología de la información – Grupo de apoyo administrativo, cuenta con un responsable para gestionar la entrega o retiro de los medios de almacenamiento de backup del sitio externo.

Registro de Respaldo de Información

- Debe existir un procedimiento formal de administración y control del Backup que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.
- Tecnología de la información – Grupo de apoyo administrativo, debe aplicar la siguiente Normativa
    - Llevar el registro de los Respaldos de Información realizada de forma Diaria.
    - Registro del retiro de los medios de almacenamiento de backup del sitio externo.
    - Registro del ingreso de los medios de almacenamiento de backup al sitio externo.
    - Inventario de los medios de almacenamiento de backup.
    - Comprobación de Integridad de la Información

- La información respaldada debe ser probada como mínimo una vez al año, asegurando que es confiable, íntegra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.
- Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.
- Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información
- Tecnología de la información – Grupo de apoyo administrativo, debe aplicar los siguientes lineamientos:
    - Restaurar anualmente, el escenario adecuado para probar las copias de respaldo de los Servidores.
    - Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.
    - Validar la integridad y accesibilidad de los medios de almacenamiento de backup por lo menos cada cuatro meses.
    - Mantener siempre una copia de la información de los Servidores, por lo menos con una antigüedad no superior a 24 horas.
- Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.
- La información de los procesos de la entidad deberá ser almacenada por los usuarios en los servidores centrales. Tecnología de la información – Grupo de apoyo administrativo es responsable de respaldar dicha información, y los usuarios son responsables de proteger dichos activos y alertar a Tecnología de la información – Grupo de apoyo administrativo cuando un activo digital de información requiera medidas especiales de protección.

Respaldo de Información para Usuarios Finales

- Toda información de PROYECTAMOS SAS que el usuario almacene en su equipo de trabajo asignado, debe ser respaldada por el usuario en las carpetas o sitios destinados para esto en los servidores de la Entidad siguiendo el procedimiento establecido de respaldo de información para los usuarios.
- Todos los usuarios son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.
- Cada líder es el responsable de validar que toda información de su proceso o subproceso este almacenada en la unidad definida para ello.

- Tecnología de la información – Grupo de apoyo administrativo, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.
- Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.
- Se debe elaborar un plan de emergencia para todas las aplicaciones que manejen información crítica de la Entidad, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- Es responsabilidad todos los funcionarios, contratistas y terceros almacenar la información crítica asociada con su labor en el servidor de archivos establecido, para garantizar que la información está siendo respaldada.
- Cumplir con la Política de respaldos y recuperación o Rollback del Manual de Políticas de Tecnología de la información – Grupo de apoyo administrativo la entidad.

LINEAMIENTOS DE EVENTOS DE AUDITORÍA

Objetivo: Asegurar que los registros de los eventos y las operaciones realizadas sobre los sistemas de información y plataforma tecnología de PROYECTAMOS SAS permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

Registro de eventos

- Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones de PROYECTAMOS SAS, deben ser registrados.
- Se deben habilitar los logs de eventos requeridos y deben ser revisados con regularidad.
- Se debe hacer copia de respaldo de información de los eventos de auditoría, ya que en caso de un incidente de seguridad de la información deben estar disponibles, la cual se mantendrá por un periodo no menor a 6 meses.

Registro del administrador y del Operador

- Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información de PROYECTAMOS SAS deben estar debidamente registradas.
- Los administradores de la infraestructura tecnología y de procesamiento de información deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal.

Sincronización de relojes

Todos los relojes de la infraestructura de procesamiento de información de PROYECTAMOS SAS, deben estar sincronizados con la hora legal colombiana.

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de PROYECTAMOS SAS.

Tecnología de la información – Grupo de apoyo administrativo es el responsable de administrar y gestionar la red de PROYECTAMOS SAS.

Tecnología de la información – Grupo de apoyo administrativo es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

- La información que sea considerada crítica o sensible deberá ser transmitida y operada de manera segura a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo de origen.
- PROYECTAMOS SAS proporciona a los funcionarios, contratistas y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por Tecnología de la información – Grupo de apoyo administrativo.
- El diseño de redes se debe hacer teniendo en cuenta que no existan puntos únicos de falla en general y en particular en seguridad; que puedan comprometer la disponibilidad de los servicios de la red, que las comunicaciones críticas puedan ser enviadas a través de transportadores (carriers) múltiples sobre diferentes rutas físicas.
- Los sistemas de cableado de energía y de comunicaciones que se utilizan en los servicios de información deben ser protegidos para evitar su intercepción o daño.
- Las direcciones de sistemas internos, las configuraciones y la información de diseño de sistemas relacionada con la red en PROYECTAMOS SAS, debe ser restringida para que los usuarios y sistemas por fuera de la red interna no puedan acceder a esta información.
- La información relacionada con el acceso a los computadores, sistemas de comunicación y las conexiones remotas externas, es considerada Pública Clasificada y no debe ser publicada en Internet, listada en directorios telefónicos, puesta en tarjetas de presentación o puesta a disposición de terceras partes.
- Los usuarios no instalarán, desinstalarán o cambiarán la configuración de sus componentes de hardware o software, accesorios internos o externos, en los elementos de TI asignados, sin la autorización previa del grupo de gestión administrativa de Sistemas
- Se deben monitorear continuamente las conexiones remotas de los computadores conectados a las redes en busca de tráfico malicioso para asegurar el uso de software aprobado, prevenir la detección e intrusión no deseadas y no aprobadas y para monitorear la actividad generada por

estos sistemas.

- En caso de tener un sistema de detección y prevención de intrusiones este debe ejecutarse continuamente en todos los servidores de Internet, servidores de bases de datos, servidores de aplicaciones, dispositivos de red y Firewalls que estén conectados a redes externas a la red de PROYECTAMOS SAS.
- Se debe provisionar de infraestructura adecuada para la realización de investigaciones a equipos informáticos en PROYECTAMOS SAS.
- Todas las máquinas conectadas a la red en PROYECTAMOS SAS deben cumplir con las configuraciones definidas.
- Todas las estaciones de trabajo conectadas a Internet a través de línea telefónica, DSL, ISDN, cable módem o cualquier sistema similar, deben tener su propio firewall personal activo y activado permanentemente.
- Todos los Firewalls de Internet, deben tener un canal de respaldo que permita a un administrador autorizado establecer una conexión, en el eventual caso de un ataque de denegación de servicio distribuida.
- Todos los servidores publicados en Internet deben ser ubicados en una zona desmilitarizada, protegida por un firewall.
- La aprobación escrita es requerida para habilitar un servicio en todos los Firewalls conectados a Internet, dado que por defecto todos los servicios son deshabilitados.
- Todos los Firewalls y sus estaciones de administración en PROYECTAMOS SAS, deben ejecutar en computadores dedicados sin otras funciones adicionales.
- La configuración de los Lineamientos de los Firewalls y los servicios permitidos serán cambiados mediante el procedimiento de control de cambios definido para PROYECTAMOS SAS.
- Todas las conexiones entre los computadores de las redes de datos en PROYECTAMOS SAS e Internet o cualquier red pública, deben incluir un firewall aprobado y los controles de acceso relacionados.
- Solo se permitirá el uso de interfaces de red externas y de protocolos que hayan sido aprobados por Tecnología de la información – Grupo de apoyo administrativo.
- El establecimiento de una conexión directa entre los sistemas en PROYECTAMOS SAS y computadores de organizaciones externas, debe seguir los procedimientos de transferencia de información.
- Todos los sistemas de computación y los segmentos de red deben cumplir con los criterios de seguridad establecidos en el proceso de seguridad de la información, pero no limitado a, cumplimiento regulatorio, la justificación de la existencia del mismo, el manejo de un firewall

aceptable, un sistema aceptable de autenticación de usuarios, un sistema aceptable de control de privilegios de usuarios, un proceso establecido de control de cambios, una definición escrita de las responsabilidades de administración del sistema y una documentación operacional adecuada. Después de esto, el sistema puede ser conectado a Intranet en PROYECTAMOS SAS.

- Se debe mantener un inventario actualizado de todas las conexiones en PROYECTAMOS SAS con redes externas.
- Las redes inalámbricas que llegara a utilizar PROYECTAMOS SAS deben estar configuradas para utilizar cifrado y autenticación fuerte en sus comunicaciones.
- Todas las comunicaciones provenientes de los dispositivos de acceso inalámbrico que brinden acceso a la red LAN en PROYECTAMOS SAS, deberán estar controladas a través de un dispositivo de control de acceso (Firewall, ACL, otros) donde se establezca la forma de acceso a la red LAN. Los cables, módems y memorias USB no deben ser utilizados para comunicaciones misionales en PROYECTAMOS SAS, a menos que se utilice un firewall y una red privada virtual con cifrado en los computadores involucrados.

Separación de las Redes

- PROYECTAMOS SAS debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se deben seguir el procedimiento para ingreso seguro a los sistemas de información para la solicitud de servicios de red.
- Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red. Se deben establecer mecanismos de autenticación seguros para el acceso a la red.
- Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

Objetivo: Asegurar la protección de la transferencia de información

Adopción de estándares generalmente aceptados para la calificación del contenido

PROYECTAMOS SAS debe adoptar y soportar los estándares generalmente aceptados para la calificación del contenido, para la protección de la privacidad en el sitio web

Intercambio de información entre aplicaciones de PROYECTAMOS SAS y otras empresas

Se deben implementar mecanismos de intercambio de información seguros entre aplicaciones de PROYECTAMOS SAS y otras empresas.

Servidores WEB que participan en intercambio de información en PROYECTAMOS SAS

Los servidores de Internet ubicados en la zona desmilitarizada (DMZ) no deben ser utilizados para almacenar información crítica o sensible de las actividades en PROYECTAMOS SAS.

Todos los servidores de comercio de Internet en PROYECTAMOS SAS que soportan comunicaciones sensibles con organizaciones externas, deben emplear certificados digitales emitidos por autoridades certificadoras (CA) reconocidas en Internet y deben utilizar cifrado para transferir información entre los sistemas involucrados.

Información que se intercambia por medios electrónicos

- Para realizar intercambio de información de propiedad de PROYECTAMOS SAS con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información.
- Toda información calificada como Pública Reservada y/o Pública Clasificada por ley, debe ser cifrada mientras esté almacenada en computadores accesibles desde Internet o desde redes externas.
- Toda información Pública Reservada y/o Pública Clasificada, debe permanecer cifrada cuando sea transmitida o almacenada en medios de respaldo y transportada.

Objetivo: Gestionar la elaboración, conservación y revisión regular de los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Registro de operaciones críticas y/o sensibles

Las operaciones críticas o sensibles de la entidad, deben ser registradas en una auditoría, para detectar y reducir el riesgo de violación o fraudes.

Manejo de Logs (Registro de eventos)

- Todos los sistemas y las aplicaciones de producción que manejen información sensible deben generar logs que evidencien cada modificación, incorporación y borrado de la información.
- Los sistemas que manejen información sensible o crítica deben además contener y activar el log sobre todos los eventos o procesos relacionados con la seguridad de acceso y que se tengan procedimientos adecuados para su explotación.
- Los logs de procesos relevantes deben de proveer información que sirva como evidencia en auditorías contribuir a la eficiencia y cumplimiento de medidas de seguridad.
- El propietario de la información debe definir la característica especial que estos logs deban incluir, de acuerdo a requerimientos internos o con autoridades externas.
- Un log debe activarse y revisarse por lo menos cada mes. Durante este período, el log no debe ser modificado, ni leído por personal no autorizado. Los logs deben ser conservados de forma tal, que no puedan ser revisados o visualizados por personas no autorizadas. Los funcionarios, contratistas y terceros deben contar con una autorización del dueño de la información en cuestión para realizar tal acceso.
- Además, todas las actividades de los usuarios que afecten el servicio deben ser trazables desde el log.
- Se deben tener registros o logs de las transacciones de los sistemas de información con información crítica o sensible en PROYECTAMOS SAS para facilitar la identificación y solución de incidencias o eventos de seguridad de la información.
- Las aplicaciones y otros manejadores de bases de datos, deben tener logs para las actividades de los usuarios y estadísticas relacionadas a estas actividades.
- Además, los mecanismos para detectar y registrar eventos de seguridad significativos, deben ser resistentes a los ataques y aun cuando el log sea apagado o modificado, esta suspensión o modificación quede registradas en el mismo.

Objetivo: Gestionar todos los incidentes de seguridad de la información reportados en PROYECTAMOS SAS, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Impacto de los incidentes

Se debe realizar la evaluación del impacto de los incidentes de seguridad de la información relevante, así como aplicar los mecanismos de atención y manejo de los incidentes.

Reporte sobre los eventos y las debilidades de la seguridad de la información

- Todos los funcionarios, contratistas, terceros y demás personal interno o externo que tenga un vínculo contractual con PROYECTAMOS SAS y que maneje activos de información, debe reportar como incidente de seguridad cualquier anomalía o mal uso de los recursos en PROYECTAMOS SAS. Todos los incidentes de seguridad de la información deben ser registrados, gestionados y documentados en sus diferentes etapas para mantener los acuerdos de niveles de servicios (ANS) negociados con los clientes y mejorar la seguridad de la información.
- Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.
- Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.
- Se debe definir el procedimiento de gestión de incidentes de seguridad de la información de la UAE
- Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.
- Se debe recolectar las evidencias (CCP, Fiscalía, Colcert, MinTic) necesarias lo más pronto posible después del reporte del incidente.
- Sólo se suministrarán pruebas técnicas para la investigación; de igual forma, la valoración de las mismas estará a cargo de la entidad competente responsable de la investigación y serán canalizadas a través de la Dirección.
- Escalar los incidentes a niveles superiores en caso de que sea requerido.
- Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.
- Para el transporte de elementos, se debe llevar la cadena de custodia. Se deben documentar todos los incidentes de seguridad reportados.
- Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

- Los incidentes de seguridad de la información asociados a falta de disponibilidad, por problemas técnicos, serán tratados como incidentes de Tecnologías de Información y serán tratados acorde a los lineamientos definidos para la gestión de incidentes de TI.

- En caso de afectar una infraestructura critica se debe aplicar el capítulo 4.3 Niveles de Alerta y Medidas de Protección y Resiliencia de las ICC del SCIT del Plan de protección para la infraestructura critica cibernética del sector Comercio, Industria y Turismo (SCIT)

- Los incidentes de seguridad de la información que involucren compromiso de la reputación o buen nombre de las personas, deben asegurar la confidencialidad más alta y la inclusión del mínimo número de personas necesario para su evaluación y ser en todo momento seguido a través de los mecanismos definidos por la Dirección.

Objetivos: Establecer los criterios de seguridad la información para la información accedida por los proveedores.

Consideraciones de seguridad en los acuerdos con terceras partes

- En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información.
- Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.
- Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivo: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de PROYECTAMOS SAS.

- PROYECTAMOS SAS debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis
- PROYECTAMOS SAS debe contar con un centro de datos alterno, para garantizar la disponibilidad de los servicios críticos de la Entidad, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.
- PROYECTAMOS SAS debe contar con una estrategia de Recuperación de Desastres que asegura la continuidad de las operaciones tecnológicas de sus procesos críticos, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento
- Para PROYECTAMOS SAS su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier evento.
- Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en los Planes de contingencias.
- Se debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica de PROYECTAMOS SAS.

Objetivo: Garantizar el acatamiento de los derechos de autor.

PROYECTAMOS SAS debe garantizar que el software que adquiera y usa la Entidad, se encuentra debidamente licenciado, considerando y acatando los derechos de propiedad intelectual; además establece:

- PROYECTAMOS SAS solo deberá adquirir software a través de fuentes conocidas y confiables, para asegurar que no se violan los derechos de autor.
- PROYECTAMOS SAS debe mantener los registros de activos apropiados, e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.
- PROYECTAMOS SAS debe mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc.
- PROYECTAMOS SAS cumple con la reglamentación de propiedad intelectual para lo cual debe implementar los controles necesarios que garanticen el respeto de dicha reglamentación.
- PROYECTAMOS SAS debe llevar a cabo revisiones con la finalidad de validar que solo hay instalados software autorizado y productos con licencia.
- No se debe permitir el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por los derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
- Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos, con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
- No se permite copiar total ni parcialmente libros, duplicar, convertir a otro formato o extraer de registros comerciales solo lo que permita la ley de derechos de autor.
- Se debe dar cumplimiento con los términos y condiciones establecidos para obtener software e información en redes públicas.
- Se debe implementar controles para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.
- Se debe hacer un control sobre el uso de software libre que hacen los usuarios, y su relación con la función que realizan.
- El software desarrollado internamente por el personal que labora en PROYECTAMOS SAS es propiedad exclusiva de la Entidad, al igual que sus documentos, 73 planos, diseños, esquema y otros desarrollos con medios de PROYECTAMOS SAS o por medio de terceros desarrollados para fines del negocio

- El Oficial de Seguridad de la Información o quien haga sus veces, autorizará la utilización de software catalogado como libre o con licencias públicas (GPL), teniendo en cuenta que no se vea afectado de ninguna manera la Entidad.

CONTROL DE CAMBIOS

Última revisión: junio 2023

- junio 2022
- junio 2021

Creado en julio 2020