PLAN DE GESTIÓN DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DE NARIÑO – CORPONARIÑO

Julio de 2018

INTRODUCCIÓN

De acuerdo con la Estrategia Gobierno Abierto , que viene siendo liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, que comprende las acciones transversales tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada en CORPONARIÑO.

Todos los servidores públicos, dentro de sus funciones, están expuestos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Como meta fundamental se orienta a gestionar los riesgos, desde su identificación hasta el monitoreo, con el reconocimiento de las causas, efectos, definición de controles y lineamientos claros para su adecuada gestión.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio. Razón por la cual, se hace necesario identificar los riesgos existentes en la Corporación, unido a la capacitación del personal para que se sigan una serie de normas y procedimientos referentes a la seguridad de la información y recursos.

1. OBJETIVOS

1.1 Objetivo General

Identificar, Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes en la Corporación Autónoma Regional de Nariño – CORPONARIÑO, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

1.2 Objetivos Específicos

Realizar el plan de trabajo concreto certificando los recursos con los que se cuentan actualmente en CORPONARIÑO para la construcción del plan de tratamiento de riesgo de seguridad y privacidad de la información

• Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

• Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.

• Proponer soluciones frente a las amenazas identificadas para minimizar los riesgos a los que está expuesta la Corporación.

• Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

• Lograr el compromiso de la Corporación para iniciar la construcción e implementación del plan de gestión del riesgo en la seguridad de la información.

• Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

• Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

2.2 LIMITACIONES

• Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Corporación Autónoma Regional de Nariño – CORPONARIÑO.

3. RECURSOS

Humano: Director General, Gestores del Proceso, Profesionales y contratistas.

Físico: Firewall, PC, Equipos Servidores, recursos web y equipos de comunicación

Financieros: A estimar

4. RESPONSABLES

- Director General de la Corporación

- Subdirectores de las dependencias de la Corporación

- Oficina de Gestión Informática y Tecnológica

5. GESTIÓN DE RIESGOS

5.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

Se ha establecido como prioridad salvar, proteger y custodiar el activo de la información, realizando un diagnóstico de los sistemas de información y los avances tecnológicos implementados en la Corporación

La Corporación Autónoma Regional de Nariño – CORPONARIÑO, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento con el Gobierno Abierto que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento a la normatividad vigente, teniendo en cuenta que una entidad sin un plan de gestión de riesgos está expuesta a perder su información; se consideran como los riesgos más comunes los ataques dirigidos al software empresarial, daños en los equipos (PC y servidores), afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación y entendiendo que el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de las actividades de la Corporación tras sufrir alguna pérdida o daño en la información de la entidad.

Por lo anterior expuesto es preciso diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

5.1.1 SITUACIÓN NO DESEADA

- Hurto de información o de equipos informáticos.

- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Manipulación indebida de información

5.2 DEFINICIONES GESTIÓN DEL RIESGO

• Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

• Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

• Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

• Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

• Materialización del riesgo: ocurrencia del riesgo identificado

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

- Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.

- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.

- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización".

Acceso a la Información Pública: derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

5.3 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

CORPONARIÑO adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.

- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.

- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.

- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Dirección General en conjunto la Oficina de Planeación y Direccionamiento Estrategico – OPDE, asignará

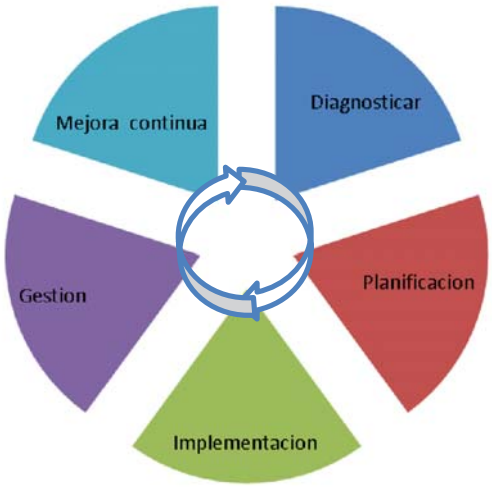
los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

6. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Nariño – CORPONARIÑO, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

Las siguientes fases de implementación del PLAN DE GESTIÓN DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar



Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

6.1 PROPÓSITO DE LA IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar soporte al modelo de seguridad de la información al interior de la Corporación.
- Preparación de un plan de respuesta a eventualidades.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

7. ACTIVIDADES

- Realizar Diagnóstico en el que se identifiquen vulnerabilidades.

- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

- Realizar la Identificación de los Riesgos.

- Valorar los riesgos.

- Visualizar donde se ubican los riesgos y su incidencia.

- Plantear un plan de tratamiento de riesgos acorde con los recursos disponibles y aprobados por las directivas de la Corporación.

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las actividades indicadas arriba, se describe a continuación que se debe desarrollar y plazos para su implementación de acuerdo a lo establecido por la Corporación.

- Revisión y/o Actualización de la actual Política de Seguridad.

- Aspectos organizativos de la seguridad de la información

- Seguridad Ligada a los recursos humanos

- Revisión del Control de acceso

- Seguridad en la operativa

- Seguridad en las telecomunicaciones

- Gestión de Incidentes de Seguridad de la Información

- Aspectos de seguridad de la información en la gestión de continuidad de las actividades.

9. CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE GESTIÓN DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN																			
MES/	AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
ACTIVIDAD	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar Diagnóstico en el que se identifiquen vulnerabilidades.																				
Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información																				
Realizar la Identificación de los Riesgos.																				
Valorar los riesgos.																				
Visualizar donde se ubican los riesgos y su incidencia.																				
Plantear un plan de gestión de riesgo en seguridad y privacidad de la información acorde con los recursos disponibles y aprobados por las directivas de la Corporación.																				
Seguimiento y control																				

10. SEGUIMIENTO y EVALUACIÓN

Al finalizar cada etapa se realizará una socialización con el Jefe de la Oficina de Planeación y Desarrollo Estratégico y la Oficina de Gestión informática y tecnológica, para presentar el informe respectivo de cada una de las actividades del avance del plan de gestión de riesgos para evaluar todos los pasos se han ido realizado.

11. ENTREGABLES

- Informe de avance para cada actividad

- Acta de Reunión.

- Plan de tratamiento de riesgo aprobado por los responsables.

- Política de Seguridad

- Productos de cada etapa

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DE NARIÑO – CORPONARIÑO

Julio 31 de 2018

INTRODUCCIÓN

La Corporación Autónoma Regional de Nariño CORPONARIÑO es una entidad de carácter público, del orden nacional, cuyo objetivo es la ejecución de las políticas, planes, programas y proyectos sobre medio ambiente y recursos naturales renovables, así como dar cumplida y oportuna aplicación a las disposiciones legales vigentes sobre su disposición, administración, manejo y aprovechamiento, conforme a las regulaciones, pautas y directrices expedidas por el Ministerio del Medio Ambiente.

En su estructura orgánica, dentro de la Oficina de Planeación y Direccionamiento Estratégico se encuentra la oficina de Gestión Informática y Tecnológica, la cual debe encargarse de mantener la funcionalidad permanente de los diferentes sistemas de información y servicios informáticos que actualmente tiene la Corporación, además de seguir con los lineamientos establecidos por las demás entidades del gobierno garantizando que las acciones tendientes al funcionamiento de la entidad cumplan la normatividad vigente.

La oficina de Gestión Informática y Tecnológica apoya todas las labores misionales y corporativas de CORPONARIÑO, que se encargan de garantizar la integridad y confiabilidad absoluta de todos los activos de información disponibles; El Plan de Privacidad y Seguridad de la Información es importante ante la posible pérdida, destrucción, robo y otras amenazas, y hace parte integral de la Estrategia de Gobierno Abierto.

CORPONARIÑO
Corporación Autonoma Regional de Nariño

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

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.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad : Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

OBJETIVOS

Objetivo General

Preservar de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos de la Corporación Autónoma Regional de Nariño – CORPONARIÑO.

Objetivos Específicos

- Formular el esquema de seguridad de la información de acuerdo a las necesidades y recursos de CORPONARIÑO

- Establecer controles para el acceso a los activos de información de la Corporación.

- Actuar conforme a la normatividad vigente a nivel Nacional las políticas de gestión y administración de activos de información de la Corporación.

- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información en la Corporación.

- Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.

JUSTIFICACIÓN

Para CORPONARIÑO, la seguridad en la información es muy importante, y ha trabajado por garantizar la calidad, disponibilidad, veracidad y confidencialidad; teniendo en cuenta que la información ahora está expuesta a amenazas y vulnerabilidades. Para el manejo de la información existe la necesidad de su aseguramiento por medio de políticas y controles, que garanticen la estabilidad y confiabilidad de la información.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno Abierto, y el conjunto de normativas que rigen al respecto, conjuntamente con la situación actual del sistema de información y los servicios tecnológicos de CORPONARIÑO, es imprescindible articular esfuerzos tendientes a ofrecer seguridad en la información, previendo las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en redes, en servicios y herramientas tecnológicas dispuestas para tal fin.

El plan de Seguridad y Privacidad De La Información comprende procesos de copias de seguridad, su protección, integralidad, restricción de acceso y demás elementos a tener en cuenta. Que beneficia a la alta dirección y a los usuarios finales que utilizan los servicios tecnológicos de la Corporación.

ALCANCE Y DELIMITACIÓN DEL PLAN

El alcance del Plan de seguridad y privacidad de la información, pretende cubrir los componentes principales del Sistema de Información Ambiental Corporativo y tecnológico de CORPONARIÑO y se actualizará permanentemente de acuerdo con los requerimientos tecnológicos e informáticos que se requieran para el funcionamiento adecuado.

La implementación de este plan se realizará con el liderazgo de la oficina de Gestión Informática y tecnológica y la Oficina de Planeación y Direccionamiento Estratégico- OPDE, y la adopción será responsabilidad de todos los Empleados de planta, administrativos y contratistas según las competencias establecidas.

SEGURIDAD DE LA INFORMACIÓN

- Seguridad Física

Se refiere a controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

De igual manera se pueden tener acciones que pongan en riesgo la infraestructura física que soporta los servicios tecnológicos en donde se alojan los activos de información de CORPONARIÑO:

- **Protección de la información y de los bienes informáticos**

El usuario o funcionario deberán reportar de forma inmediata LA OFICINA DE Gestión Informática y Tecnológica, cuando detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, el funcionario o contratista tiene la obligación de proteger las unidades de almacenamiento que se encuentre bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

Es responsabilidad del funcionario o contratista evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo que tenga asignados.

- **Protección y ubicación de los equipos**

Los Empleados de planta, administrativos y contratistas no deben mover o reubicar los equipos de cómputo, instalar o desinstalar software no autorizado, ni retirar sellos de los mismos, sin autorización, en caso de requerir este servicio deberá solicitarlo a la oficina de Gestión Informática y Tecnológica de la Corporación.

El equipo de cómputo asignado, deberá ser de uso exclusivo de las funciones de los Empleados de planta, administrativos y contratistas de CORPONARIÑO.

Es responsabilidad de los Empleados de planta, administrativos y contratistas almacenar su información únicamente en la partición del disco duro diferente a la destinada para archivos de programa y sistemas operativos o indicada por el personal a cargo.

El funcionario o contratista no podrá abrir o destapar los equipos de cómputo, sólo personal calificado de la oficina de Gestión Informática y Tecnológica puede realizar este trabajo

Se debe evitar colocar objetos encima del equipo de cómputo u obstruir las salidas de ventilación del monitor o de la CPU, así mismo el cuidado de los equipos de impresión de la Corporación.

- Mantenimiento de equipos de cómputo

Únicamente el personal autorizado podrá llevar a cabo los servicios y reparaciones al equipo informático.

Los Empleados de planta, administrativos y contratistas deberán asegurarse de respaldar en copias de seguridad la información relevante cuando el equipo sea enviado a reparación, previniendo así la pérdida involuntaria de información derivada del proceso de reparación.

El mantenimiento preventivo de los equipos de cómputo de la Corporación (servidores, computadores de escritorio, computadores portátiles, impresoras, escáner, circuito se realizaran para la Corporación y Centros Ambientales por lo menos 2 veces al año.

- Perdida de equipo

El funcionario o contratista que tenga bajo su responsabilidad o asignado algún equipo es responsable de su uso y custodia; en consecuencia responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

- Software identificado en CORPONARIÑO:

Identificados bajo el estándar ISO/IEC 27000: Norma técnica con la descripción general y vocabulario sobre la administración de sistemas de seguridad de la información.

SISTEMA DE INFORMACIÓN	FUNCIÓN
PCT	Es el sistema de información administrativa y financiera con el que cuenta la Corporación Autónoma regional Nariño. Este es un sistema gráfico integrado modular, es de fácil manejo y muy flexible para ajustarse a los cambios en la normatividad del sector público, al ser un sistema Cliente - Servidor se encuentra instalado en los equipos de los usuarios finales que así lo requieren. El sistema se encuentra funcionando, utilizado para gestionar operaciones de ingresos, gastos, pagos y demás transacciones derivadas de las áreas de tesorería y contabilidad, demanda soporte especializado Oracle para solucionar casos de error, ajustes y desarrollo de nuevas funcionalidades acorde con los requerimientos presentados por los responsables del módulo.
Página WEB	Portal corporativo desarrollado en WordPress, es administrado por un ingeniero de sistemas contratista, adscrito al proyecto de gestión informática y tecnológica de Corponariño. CORREO CORPORATIVO Se utiliza para la comunicación de los Empleados de planta, administrativos y contratistas el correo corporativo web mail corponarino, que se encuentra Correo institucional – Corponariño:

	http://webmail.corponarino.gov.co/, cada dependencia y funcionario autorizado tiene una usuario y contraseña para acceder al mail. Este correo es interno en la Corporación, algunos correos se ha re direccionado a Gmail para funcionarios que necesitan utilizarlo externamente.
INTRANET	Plataforma web interna, desarrollada en WordPress, se encuentra actualizada tiene acceso desde el portal web. Instalada en un servidor local Linux, es utilizada frecuentemente para consultar la documentación del Sistema Integrado de Gestión, además se puede hacer consultas de ccertificaciones laborales del personal de planta de la Corporación.
VITAL	Plataforma Ventanilla Integral de Trámites Ambientales en Línea VITAL, herramienta utilizada para registrar, gestionar y consultar los trámites ambientales en línea de la Corporación, para dar cumplimiento al decreto 2041 de 2014, plataforma desarrollada y administrada por la Autoridad Nacional de Licencias Ambientales ANLA. Las solicitudes se registran en la plataforma VITAL, se digitalizan y cargan los soportes documentales. Se actualiza con frecuencia debido a la rotación de personal y sin embargo se identifican trámites sin finalizar o incompletos en ocasiones.

SILA	Plataforma Sistema de Información para la Gestión de Trámites Ambientales SILA, es un Software utilizado para la Gestión de Trámites a la medida de las Autoridades Ambientales. El cual permite: * Consulta y descarga de documentos enviados por los usuarios solicitantes. * Expedición de Actos Administrativos. * Expedición de Oficios de Requerimientos. * Programación de Visitas Técnicas.
Bases de datos en Excel (Gestión de Tramites Servicios Ambientales-Licencias Ambientales)	Esta información se encuentra depositada en VITAL.
Bases de datos en Excel (Gestión de Tramites Servicios Ambientales-Concesiones de Agua)	Esta información se encuentra depositada en VITAL.
Bases de datos en Excel (Gestión de Tramites Servicios Ambientales-	Esta información se encuentra depositada en VITAL.

Aprovechamientos Forestales)	
Bases de datos en Excel (Gestión de Tramites Servicios Ambientales - Registro del libro de operaciones forestales)	Esta información se encuentra depositada en VITAL.
Herramientas SIG (ArcGis, Quantum GIS,	ArcGIS53 es llamado el conjunto de productos de software en el campo de Sistemas de Información Geográfica o SIG, bajo el nombre genérico ArcGIS se reúnen diferentes aplicaciones para la edición, tratamiento, diseño, impresión y análisis de la información geográfica, Quantum GIS - QGIS es un Sistema de Información Geográfica SIG de Código Abierto licenciado bajo GNU - General Public License.
Documentación Sistema Integrado de Gestión	Conjunto de documentos asociados a los procesos del Sistema Integrado de Gestión. Los archivos se encuentran almacenados en el servidor bajo linux (10.0.0.106), que soporta la intranet corporativa, los cuales se vinculan desde el mapa de procesos del sistema hasta la documentación que se maneja a

	nivel interno dentro la Corporación.
Bases de datos banco de proyectos	Instrumento muy utilizado para llevar el seguimiento a los proyectos que formula la Corporación ante diferentes orígenes de financiación y los que presentan los demás centros ambientales que se encuentran en el Departamento de Nariño para la asignación de recursos.
SPARK	Spark es un cliente de mensajería instantánea ideal para crear una red interna, la mayor diferencia que tiene Spark con el resto de programas similares salta a la vista al primer vistazo, su interfaz es mucho más agradable, amigable y fácil de utilizar. Tiene un cómodo sistema de envío de archivos con barra de progreso, simplemente arrastrar y soltar; salas de chat para múltiples personas. COMUNICACIÓN INTERNA CORPONARIÑO, mensajería Instantánea. Para la mensajería instantánea se utiliza el programa Spark, que es un cliente de mensajería instantánea ideal para crear una red interna y también para todos aquellos que se comuniquen a través de otros clientes basados en Jabber. Cada usuario autorizado puede ingresar para comunicarse entre las dependencias y centros ambientales de manera efectiva.
Bases de datos en Excel Permisos de vertimientos	Esta información se encuentra depositada en VITAL.

SINCA	Sistema de Normalización y Calidad Ambiental, se encuentra actualizado y funcionando, utilizado para gestionar los trámites de permisos, autorizaciones y licencias ambientales. A partir de la implementación de VITAL, el sistema no fue utilizado para registrar nuevos trámites; sin embargo, debían registrarse las actuaciones de seguimiento de trámites anteriores a VITAL.

RESPALDO DE LA INFORMACIÓN

Las copias de seguridad que están disponibles en la Corporación son las siguientes:

- **Discos Duros**: Dispositivos de almacenamiento internos y externos asignados a Empleados de planta, administrativos y contratistas, se realiza en ellos los Backup realizados manualmente cada vez que crea necesario y reposará bajo su custodia, allí el usuario almacenará la información que el considere vital.

- **Carpetas Compartidas**: Se destina de un servidor, donde se crea una carpeta por cada dependencia, y carpetas a los usuarios que lo requieran, con un nombre de usuario de red y solamente este usuario tendrá todos los permisos para guardar directamente la información que considere necesaria.

- **Servidor**: Es el espacio destinado del servidor para el usuario y poder colocar información en las carpetas compartidas.

- **Discos de Almacenamiento**: Se realiza diariamente una copia desde el servidor donde se almacenan las carpetas compartidas, estará bajo la custodia

únicamente del Ingeniero de Sistemas.

Para realizar un análisis de todos los elementos de riesgos a los cuales están expuestos los equipos informáticos y la información procesada por CORPONARIÑO, se iniciara describiendo los activos que se pueden encontrar dentro de las tecnologías de información y la comunicación de la Corporación:

ACTIVOS SUSCEPTIBLES DE DAÑO

El Personal, Hardware, Software, Periféricos, Datos, información, Documentación Física y magnética, Suministro de energía eléctrica y Suministro de telecomunicaciones

Posibles daños

• Dificultad de acceso a los recursos debido a problemas físicos en las instalaciones.

• Inconvenientes de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información.

• Divulgación de información a instancias fuera de la Corporación y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

FUENTES DE DAÑO

• Acceso no autorizado.

• Ruptura de las claves de acceso al sistema informático.

• Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario).

• Fallas de Personal (Enfermedad, Accidentes, Renuncias, Abandono de su puesto de trabajo).

• Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red Switches, cableado de la Red, Router, FireWall).

• Falla en el servicio del proveedor de Internet.

IDENTIFICACIÓN DEL RIESGO

Riesgo: Perdida de la confidencialidad e integridad de la información por faltas en la seguridad informática en beneficio de un particular

Causas:

-Generación de información confusa o errada sobre los temas de la entidad.

-Falta de unidad de criterio sobre el manejo de los temas

-Incumplimiento en la entrega de los productos finales.

Riesgo: Pérdida de Información.

Causas:

- Falta de capacitación para implementar actualizaciones normativas y procedimentales

- Cambio de la normatividad relacionada con TIC que impliquen modificación de las actividades.

- Falencias en la generación de copias de seguridad de los equipos servidores.

- Falencias en los controles de seguridad informática.

- Fallas y errores en la infraestructura tecnológica.

Una vez realizada la identificación de riesgos, se tiene que es posible la presencia de:

• Incendios.

• Robo común de equipos y archivos.

- Falla en los equipos.
- Virus informático.
- Fenómenos naturales.
- Accesos no autorizados.
- Ausencia del personal de sistemas.
- Bajas Eléctricas

Minimización del riesgo

Teniendo en cuenta, corresponde al presente Plan de Seguridad Informática del CORPONARIÑO minimizar estos índices con medidas preventivas y correctivas sobre los riesgos más relevantes.

- **FALLA EN LOS EQUIPOS**

GRADO DE IMPACTO: MODERADO

La falla en los equipos pocas veces se debe a falta de mantenimiento y limpieza.

El daño de equipos por fallas en la energía eléctrica, algunos equipos no cuentan con dispositivos que amplíen el tiempo para apagar el equipo correctamente

Equivocaciones de forma involutaria con respecto al menjo de información, software y equipos.

Se presentan dudas e inquietudes en el manejo de los equipos de cómputo por parte de Empleados de planta, administrativos y contratistas.

ACCIÓN PREVENTIVA

Realizar mantenimiento preventivo de equipos de cómputo e impresoras anualmente, según cronograma.

El administrador de la red debe asignar permisos y privilegios a cada usuario de acuerdo a sus funciones y/o competencias.

Capacitar en temas de informática básica y asistencia como soporte para la realización de las actividades.

- **ACCIÓN DE VIRUS INFORMÁTICO**

La Corporación cuenta con software antivirus NOD 32, pero no se realiza una actualización de forma inmediata a su expiración en cuanto a las licencias y bases de datos.

Sólo la oficina de Gestión Informática y tecnológica es la encargada de realizar la instalación del software antivirus en cada uno de los equipos.

ACCIÓN PREVENTIVA.

El antivirus poseen problemas por expiración de las licencias, por ello se ha solicitado la adquisición de licencias y de forma periódica se realiza el mantenimiento de software respectivo.

- **ACCESOS NO AUTORIZADOS**

Se controla el acceso al sistema de red mediante un administrador con su respectiva clave, la asignación de los usuarios se realiza en Gestión Informática y Tecnológica con el visto bueno del gestos de la dependencia.

Se borran los usuarios del personal que se retira de la Corporación tan pronto como se tenga el aviso por parte de la administración.

Las contraseñas de inicio de sesión a las aplicaciones y programas de Corponariño son exclusivas de Empleados de planta, administrativos y contratistas, dichas contraseñas se mantienen vigentes en tanto el personal esté vinculado a la Corporación.

- **MIKROTIK**

Mikrotik te brinda la posibilidad de gestionar varias aplicaciones de la Corporación, ya sea instalando el software en PC o entre ellas:

-Enlaces inalámbricos

- Identificación y priorización de tráfico. Control de tráfico, Mikrotik puede aplicar muchas reglas para la optimización de la ISP.

- Firewall NAT. Se utilizan aplicaciones de última tecnología para impedir que alguien pueda entrar a la red sin autorización.

- Servidor de VPN. Todas las terminales funcionan como una red única.

- Control de prioridad P2P. Se controla el tráfico P2P.

- Tareas programadas.

RECUPERACIÓN Y RESPALDO DE LA INFORMACIÓN

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Corporación, Se establece los procedimientos relativos a: Sistemas e Información, Equipos de Cómputo, Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

a) Sistemas de Información

La Corporación cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backups.

b) Equipos de Cómputo

Se debe tener en cuenta el inventario de Hardware, impresoras, scanner criterios sobre identificación y protección de equipos:

• Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.

• Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en

caso de evacuación o buscar información importante, en este caso aplica los servidores de aplicaciones y carpetas compartidas.

• Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la corporación.

GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO (BACKUPS)

En el procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

• Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores, estas copias de seguridad deben realizarse al menos una vez a la semana.

• Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.

• Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas, estas se harán en un disco duro exclusivo para tal fin.

• Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.

• Se utilizará el programa WINRAR u otra aplicación GNU-GLP o de prueba para comprimir el listado de archivos o carpetas a respaldar.

CORPONARIÑO
Corporación Autonoma Regional de Nariño

RECOMENDACIONES PARA EQUIPOS DE CÓMPUTO

Poner especial atención a las actualizaciones del navegador web, el sistema operativo como Windows es propenso a fallos, riesgo que puede ser aprovechado por delincuentes informáticos, frecuentemente se liberan actualizaciones que solucionan dichos fallos.

• Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, nos 'ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

• Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el proceso de Gestión de TIC en antivirus, Outlook, office, navegadores y otros programas.

• Tener el antivirus actualizado con frecuencia. Escanear con el antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados por internet.

• Estar pendiente de la fecha de caducidad de la licencia con el fin de renovarla inmediatamente tan pronto esta se cumpla.

• Es recomendable tener instalado en los equipos algún tipo· de software anti-spyware para evitar que se introduzcan en el equipo programas espías destinados a recopilar información confidencial sobre el usuario.

• Para prevenir infecciones por virus informático, los usuarios de CORPONARIÑO no deben hacer uso de software que no haya sido proporcionado y validado por La Gestión Informática y Tecnológica.

• Los Empleados de planta, administrativos y contratistas con asesoría de los profesionales de la oficina de Gestión Informática y Tecnológica de CORPONARIÑO deben verificar que la información y los medios de

almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado antes de ejecutarse.

• Ningún funcionario, contratista o personal externo, podrá descargar software, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la oficina de Gestión Informática y Tecnológica.

NAVEGACIÓN EN INTERNET Y LA UTILIZACIÓN DE CORREO ELECTRÓNICO

Navegue por páginas web seguras y de confianza, para identificarlas verifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad, extreme la precaución si va a facilitar información confidencial a través de internet.

Utilizar contraseñas seguras, es decir aquellas compuestas por ocho caracteres, como mínimo y que combinen letras, números y símbolos.

Programas de acceso remoto. A través de internet y mediante estos programas (Teamviewer), es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la seguridad de su sistema.

Tratamiento de su correo electrónico, ya que este se ha convertido en una de las formas más utilizadas para introducir código malicioso, llevar a cabo estafas, introducir virus, etc.

USO DE DISPOSITIVOS EXTRAÍBLES

El Funcionario o usuario que tenga asignados estos tipos de dispositivos será responsable del buen uso de ellos.

• La persona encargada de administrar cada equipo deberá velar por el uso adecuado de dispositivos de almacenamiento externo, como Pen Orives, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.

• Cada vez que se inserte un dispositivo externo a la red de la corporación, deberá ser analizado con el software del antivirus.

RECURSOS

1. Activos físicos y tecnológicos

2. Servidores.

3. Firewall.

4. Ingenieros en configuración de firewall, TCP/IP, ingenieros en soporte.

5. Conectividad permanente a Internet.

6. Dispositivos de almacenamiento.

7. Infraestructura corporativa.

8 .Recurso humano: Directivos, Funcionarios y/o contratistas grupo sistemas Gestión Informática y Tecnológica).