PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION VIGENCIA 2022

CONTRALORIA GENERAL DEL DEPARTAMENTO
ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA

Enero 2022

Avenida Francisco Newball, Edificio OCCRE piso 3 - San Andrés Isla
Tel.: 51 25190 - 51 20189 - Fax: 51 22465
Correo Electrónico: contraloria@contraloriasai.gov.co
Página Web: www.contraloriasai.gov.co

INTRODUCCIÓN

Establecer acciones preventivas y correctivas es de vital importancia para garantizar la continuidad de las operaciones en la entidad a nivel de sistemas de información y comunicaciones, por lo tanto, se deben aplicar medidas de seguridad encaminadas a proteger los recursos informáticos, definiendo pautas en la actuación y su uso.

Así mismo es de vital importancia definir pautas a seguir que permitan prevenir y permitir recuperar en el menor tiempo posible y de manera adecuada la información en caso de presentarse es los sistemas de información, equipos de cómputo y red de datos.

El propósito del siguiente plan es establecer los lineamientos que en materia de seguridad y privacidad de la información requiera la Contraloría Contraloria General del Departamento Archipiélago y formular políticas, estrategias y parámetros necesarios para evitar vulnerabilidades que afecten los Sistemas de Información.

BASE LEGAL

Normatividad Externa

- Ley Estatutaria 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013: “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública

- Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

DEFINICIONES

Activo: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Aplicaciones críticas: Son las aplicaciones o sistemas de información que reciben este término porque previamente se encuentran clasificados como vital o necesarias para el buen funcionamiento de los procesos y procedimientos misionales.

Brecha: Término que se utiliza para denominar la diferencia que se observa entre el mecanismo de seguridad que existe y la situación ideal para evitar que germinen vulnerabilidades que impacten el negocio de la Entidad.

Buenas prácticas: Son lineamientos que contiene los principios básicos y generales para el desarrollo de los productos o servicios de la organización para la satisfacción al cliente.

Ciclo de vida de la información digital: Se refiere a la clasificación y almacenamiento de la información; siendo necesario tener en cuenta los requisitos técnicos y legales; así como tener claro los conceptos de disponibilidad y velocidad que depende de la misma clasificación que varía conforme su valor con el tiempo.

Clasificación de las aplicaciones: Las aplicaciones se clasifican conforme los procesos de la entidad y son: Misional, Estratégico y de Apoyo.

Clasificación de la información: Proceso formal que se utiliza para ubicar el nivel a la información de la Entidad con el fin de protegerla; previa estructura de valoración en atención al riesgo que se presume existe si hay una divulgación no autorizada. Generalmente la información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

Clientes: Persona natural o usuario que recibe un producto Institucional. El cliente puede ser interno o externo a la organización.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

Corriente eléctrica regulada: Se utiliza para regular o mantener el voltaje de la red eléctrica para que no afecte el funcionamiento de los recursos TIC de la Entidad.

Dato: Es una letra, número o símbolo que tiende a convertirse en información.

Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Documento: Es el medio físico que contiene la información que se quiere transmitir.

Dueño de la información: Es cualquier persona que es propietaria de la información y tiene la responsabilidad de custodiarla.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o reducción de la calidad del servicio.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas,

narrativas o audiovisuales, y que es guardada en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Información Digital: Cuando la información está almacenada en un medio magnético porque cuando se imprime se convierte en documento físico y en este último caso existe en el SGC la dependencia que define los lineamientos, normas, guías y estándares.

Información sensible: Es la tipificación que recibe la información que no se considerada de acceso público como por ejemplo ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Política TIC: Documento que contiene los lineamientos que define la organización para reglamentar el desarrollo de los proyectos y recursos TIC de la Entidad; como las acciones que deben permanecer en el tiempo para alcanzar los objetivos de su negocio.

Política de seguridad: Es el documento de normas y lineamientos de seguridad de la información que define la Entidad para evitar que surja vulnerabilidades que puede afectar el negocio de la Entidad.

Procesos críticos: Concepto que se utiliza para definir el conjunto de actividades o eventos que se ejecutan bajo ciertas circunstancias que inciden en los productos misionales de la entidad y en la satisfacción de los clientes.

Proveedores: Negocio o empresa que ofrece servicios a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, alojamiento de aplicaciones web etc.

Propietario de la información: Se utiliza para denominar a la persona autorizada para organizar, clasificar y valorar la información de su dependencia o área conforme al cargo de la estructura organizacional de la Entidad.

Repositorio de documentos: Sitio centralizado donde se almacena y mantiene información digital actualizada para consulta del personal autorizado.

Requerimiento: Necesidad de un servicio TIC que el usuario solicita a través del mecanismo definido por la organización en los procedimientos normalizados.

Servicio: Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de

Hardware y soporte tanto de software como de hardware; así como de la Plataforma Tecnológica.

Servicios TIC: El concepto de Servicio TIC consiste en dar soporte, de forma integrada y personalizada, a todas estas herramientas que necesita hoy en día el profesional de empresa para realizar su trabajo. Los elementos del Servicio TIC.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TIC: Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, en la actualidad no solo una computadora hace referencia al procesamiento de la información. Internet forma parte de ese procesamiento que, quizás, se realice de manera distribuida y remota. El procesamiento remoto, además de incorporar el concepto de telecomunicación, hoy día hace referencia a un dispositivo como un teléfono móvil o una computadora ultra-portátil, con capacidad de operar en red mediante Comunicación inalámbrica.

Usuario: Persona que utiliza los recursos TIC y que interactúan de forma activa en un proceso, secuencia, código etc.

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la Duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No Repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

POLÍTICAS DE SEGURIDAD

Acceso a la Información

Todos los funcionarios públicos y contratistas que laboran para la Contraloría General del Departamento Archipiélago deben tener acceso sólo a la Información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Contraloría General del Departamento Archipiélago, es responsabilidad Contralor General del Departamento o Contralor Auxiliar, autorizar el acceso sólo indispensable a la información y a los equipos de cómputo, de acuerdo con el trabajo realizado por estas personas, previa justificación. Todas las prerrogativas para el uso de los sistemas de información de la entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la entidad. Terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Seguridad de la Información

Los funcionarios públicos, y contratistas de la Contraloría General del Departamento Archipiélago son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. Los funcionarios públicos y contratistas no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas. Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario y contratistas de la Contraloría General del Departamento Archipiélago deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información están en la obligación de reportar el hecho a la Contraloria Auxiliar. Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

Seguridad para los Servicios Informáticos
El sistema de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de cada competencia funcionario y de las actividades contratadas en el caso de los contratistas.

Seguridad en Recursos Informáticos
Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos y contratistas de la Contraloría General del Departamento Archipiélago son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales. Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Seguridad en Comunicaciones
Las direcciones internas (IP), topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser considerados y tratados como información confidencial y no pueden ser modificadas sin previa autorización de la persona encargada de administrar el recurso informático de la Entidad.
Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización. Los computadores de la Contraloría General del Departamento Archipiélago se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del área de sistemas. Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada. Este cifrado de información aplica únicamente para la información que es enviada anualmente a la Auditoría General de la República a través del SIREL, utilizando el certificado de firma digital entregado por Certicámara, el cual consta del token y la contraseña respectiva.

Seguridad para Usuarios Terceros
Los dueños de los Recursos Informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes. Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de Contraloría General del Departamento Archipiélago para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por el funcionario delegado por Contralor General del Departamento. Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el jefe inmediato. La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el Contralor General del Departamento con el fin de no comprometer la seguridad de la información interna de la entidad.

Software Utilizado
Todo software que utilice la Contraloría General del Departamento Archipiélago será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos. Todo el software de manejo de datos que utilice la Contraloría General del Departamento Archipiélago dentro de su infraestructura informática, deberá contar con las técnicas apropiadas para garantizar la integridad de los datos. Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos y contratistas de las implicaciones que tiene el instalar software ilegal en los computadores de la Contraloría General del Departamento Archipiélago. Está prohibido el uso de software ilegal dentro de la Contraloría General del Departamento Archipiélago, así mismo la descarga de software a través de Internet y su posterior instalación. El funcionario encargado de administrar el recurso informático de la entidad, está autorizado para monitorear periódicamente los equipos y en los casos de encontrar software instalado no licenciado por la Entidad, llevar a cabo las acciones correctivas e informar al Contralor Auxiliar las irregularidades encontradas.

Actualización de Hardware
Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área de sistemas. La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado. Los equipos de cómputo (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del funcionario del Area de Sistemas.

Almacenamiento y Respaldo
La información que es soportada por la infraestructura de tecnología informática de la Contraloría General del Departamento Archipiélago deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad. Las copias de seguridad se realizarán de acuerdo con los procedimientos establecidos. El Jefe del área dueña de la información, con la asesoría de la funcionario del Area de Sistemas de la Contraloría General del Departamento Archipiélago, definirán la estrategia a seguir para el respaldo de la información. Los funcionarios públicos son responsables de los respaldos de su información en los computadores, siguiendo las indicaciones técnicas dictadas.

Contingencia
La administración de la Entidad debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

Seguridad Física
Los equipos de cómputo (PCS, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa. Los funcionarios públicos se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras, ventiladores y en general cualquier equipos que generen

caídas de la energía. Los particulares en general no están autorizados para utilizar los recursos informáticos de la entidad.

Escritorios y Computadores Limpios
Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, s, Memorias Flash (USB), con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

Es responsabilidad de los funcionarios públicos, contratistas y pasantes de la Contraloría General del Departamento Archipiélago, mantener en buen estado los equipos de cómputo asignados para el desempeño de las labores diarias, igualmente se recomienda no consumir alimentos y bebidas que accidentalmente puedan ser derramadas sobre los computadores, periféricos, documentos y otros elementos, con el fin de evitar daños irreparables en los mismos.

Administración de la Seguridad
Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al Contralor Auxiliar de la Entidad. Los funcionarios públicos y contratistas de la Contraloría General del Departamento Archipiélago que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos computacionales. La implementación debe ser consistente con las prácticas establecidas por el Area de Sistemas. Los funcionarios que realicen labores de administración del recurso informático de la Entidad, divulgarán, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará al Contralor, los casos de incumplimiento con copia al Contralor Auxiliar y al jefe de la Oficina de Control Interno, para que estos tomen las medidas correctivas correspondientes.

Generales

Todo lo no expresamente permitido está prohibido al funcionario público (Art. 6 Constitución política de Colombia).

- Toda Información Contenida, Procesada o Generada en los equipos de cómputo es propiedad de la Contraloría General del Departamento Archipiélago.

- El usuario es el UNICO responsable de la información contenida en el o los PC'S asignados para ello. El usuario deberá determinar el grado de importancia y el tiempo que se debe conservar la información que amerita copias de seguridad, entre esta información tenemos la siguiente: Hojas de Excel, Documentos tipo Word. Carpeta de correo personal, Manejo de contactos para correo, Software de carácter no institucional.

- Antes de realizar un Backups verifique el tamaño de los documentos a copiar y compáralo con el del medio en donde va a almacenar la copia, con el fin de determinar cuántos medios necesitará para que la copia quede completa.

- Verifique que el medio en donde va a copiar esté en buenas condiciones físicas, por ejemplo, que el CD o DVD no esté con rayones, esté en buen estado y se pueda leer. De esta manera, asegura que la información posteriormente pueda ser recuperada.

- No deje visible sus contraseñas de correo, red y archivos, porque pueden ser utilizadas por otras personas alterando o dañando su información.

- No permita que personal externo opere su información, tampoco comparta sus contraseñas.