Resolución N° 2016500001964

Por medio de la cual se adopta el Manual de Seguridad de la Información para la Contraloría General de Antioquia"

EL CONTRALOR GENERAL DE ANTIOQUIA

En ejercicio de sus atribuciones legales y constitucionales, en especial las conferidas por la Ley 330 de 1996, la Ordenanza 27 de 1998.

CONSIDERANDO

a). La Contraloría General de Antioquia es una Entidad de carácter técnico con autonomía presupuestal y administrativa, de conformidad con lo que dispone la Constitución Política de Colombia en el Artículo 267.

b). Según el numeral 9° de la Ordenanza 27 de 1998, el Contralor General de Antioquia tiene como función dictar y ejecutar los actos administrativos necesarios para el funcionamiento de la Entidad.

c). La Ley 872 de 2003, establece la obligatoriedad de poner en funcionamiento el Sistema de Gestión de la Calidad en la Rama Ejecutiva del Poder Público, y en otras entidades prestadoras de servicios, norma que se hizo extensiva a la Contraloría General de Antioquia, mediante Ordenanza 24 de 2003.

d). El Decreto Nacional 2145 de 1999, establece en su Artículo 13 como responsabilidad de todos los niveles y áreas de la organización en ejercicio del autocontrol, documentar y aplicar los métodos, metodologías, procesos y procedimientos y validarlos constantemente con el propósito de realizar los ajustes y actualizaciones necesarias de tal manera que sean el soporte orientador fundamental, no sólo para el cumplimiento de sus funciones asignadas, sino para el cumplimiento de las metas y objetivos establecidos tanto en el Plan Estratégico Corporativo como en los Planes de Acción.

e). La Arquitectura TI Colombia le permite al Estado ser más eficiente al unir los esfuerzos de sus entidades y se basa en el Marco de Referencia que alinea la gestión TI con la estrategia del Estado.

f). Todas las entidades públicas deben adoptar el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI como el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno en línea.

g). Marco de Referencia es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno en línea, con él se busca habilitar las estrategias de TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la Seguridad y la privacidad de la Información.

h). Los ejes temáticos de la estrategia de gobierno en línea esta divididos en:

TIC para el Gobierno Abierto: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC.

TIC para servicios: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.

TIC para la gestión: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa.

Seguridad y privacidad de la información: Busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

i). La Estrategia de Tecnología de Información -TI- se creó como respuesta a la necesidad del Estado Colombiano de disponer de un modelo para la gestión de la Tecnología y de la Información encaminado a maximizar los beneficios y ofrecer mejores servicios a las personas y a las instituciones, de manera más eficiente y transparente.

j). El Manual de Seguridad de la Información para la CGA se constituye como uno de los elementos del ámbito de Direccionamiento Estratégico de la Estrategia TI y para el cumplimiento de la Estrategia de Gobierno en Línea.

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el Manual de Seguridad de la Información, concordante con los siguientes lineamientos: El Decreto 1078 de 2015,"*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*"; El Modelo de Seguridad para las entidades del Estado del Ministerio de las Tecnologías de la Información y las Comunicaciones, donde entrega una guía para construir el Sistema de Gestión de Seguridad de la Información (SGSI).

CONTRALORÍA GENERAL DE ANTIOQUIA

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Responsable de Aprobación:

Sergio Zuluaga Peña,
Contralor General de Antioquia

Responsable de Revisión:
Juan Carlos Peláez Serna,
Jefe Oficina Asesora de Planeación

Revisión de Documentación:
Patricia Carvajal Vargas,
Contralora Auxiliar Planeación

Responsables de la elaboración:

LUIS CARMELO CATAÑO CATAÑO

Director de Sistemas de Buen Gobierno y las TIC

DIEGO ALONSO GARCIA GÓMEZ

Profesional Especializado

NANCY ESTELLA GARCÍA OSPINA

Profesional Universitario

M-H07-01

Diciembre de 2016

Contenido

Introducción

El Desarrollo del 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 y el tamaño y estructura de la Contraloría General de Antioquia – CGA.

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 la CGA.

Objetivo

El objetivo de este documento es establecer las Políticas en Seguridad de la Información de la CGA de acuerdo a los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

Alcance

Políticas en Seguridad de la Información cubren todas las áreas de Gestión de la entidad las cuales deben ser acatadas tanto por la alta dirección, funcionarios y terceros que laboren o tengan relación con la CGA, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Definiciones

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).

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).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (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)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así

como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

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).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (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.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

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 consecuencias. (ISO/IEC 27000).

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).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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. (ISO/IEC 27000).

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

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Normatividad

El Manual de Políticas de Seguridad de la Información se ciñe a la normatividad legal vigente colombiana y de las Buenas Prácticas establecidas por la ISO 27000.

Año Emisión	Emisor	Norma	Asunto
2015	Presidencia de la República	Decreto 1078 del 26 de mayo de 2015	*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*
2006	ICONTEC	Norma Técnica Colombiana NTC-ISO/IEC 27001	Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos
2013	Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.	ISO/IEC 27002:2013	Mejores prácticas en la gestión de la seguridad de la información
2007	IT Governance Institute	Marco de Trabajo COBIT 4.1	Estándares internacionales para la dirección y control de la tecnología de la información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Modelo Guía	Modelo de Seguridad y Privacidad de la Información

2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Guía No. 2	Elaboración de la política general de seguridad y privacidad de la Información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Guía No. 3	Procedimientos De Seguridad De La Información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Guía No. 8	Controles de Seguridad y Privacidad de la Información

Con apoyo en

Guías (http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html) para construir el Sistema de Gestión de Seguridad de la Información (SGSI) para las entidades del Estado. (Ministerio de las Tecnologías de la Información y las Comunicaciones)

Manual de Políticas de Seguridad de la Información (https://www.icetex.gov.co/dnnpro5/en-us/elicetex/manualesdelaentidad.aspx) (Instituto Colombiano de Crédito y Estudios Técnicos en el Exterior).

Política Global De Seguridad de la Información

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

La Contraloría General de Antioquia, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

→ Minimizar el riesgo de los procesos misionales de la entidad.

→ Cumplir con los principios de seguridad de la información.

→ Cumplir con los principios de la función administrativa.

→ Mantener la confianza de los funcionarios, contratistas y terceros.

→ Apoyar la innovación tecnológica.

→ Implementar el sistema de gestión de seguridad de la información.

→ Proteger los activos de información.

→ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

→ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Contraloría General de Antioquia

→ Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de La Contraloría General de Antioquia y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

Políticas de seguridad que soportan el SGSI de La Contraloría General de Antioquia:

1. La Contraloría General de Antioquia ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los

requerimientos regulatorios que le aplican a su naturaleza.

2. Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistas o terceros**.

3. La Contraloría General de Antioquia **protegerá la información** generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

4. La Contraloría General de Antioquia **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. La Contraloría General de Antioquia **protegerá su información** de las amenazas originadas por parte **del personal**.

6. La Contraloría General de Antioquia **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

7. La Contraloría General de Antioquia **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. La Contraloría General de Antioquia **implementará control de acceso** a la información, sistemas y recursos de red.

9. La Contraloría General de Antioquia garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. La Contraloría General de Antioquia garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. La Contraloría General de Antioquia **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. La Contraloría General de Antioquia garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo

establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Compromiso De La Alta Dirección

La Alta Dirección de la CGA aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad, teniendo en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales y sus procesos misionales.

Alta Dirección de la entidad demuestran su compromiso a través de:

→ La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.

→ La promoción activa de una cultura de seguridad.

→ Facilitar la divulgación de este manual a todos los funcionarios de la entidad.

→ El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.

→ Monitoreo para determinar la efectividad y cumplimiento de las políticas aquí mencionadas.

→ Asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones

Procedimientos De Seguridad Y Privacidad De La Información[1]

Política De Seguridad Del Recurso Humano

En este dominio relacionado con el personal que labora dentro de la entidad, se pueden definir los siguientes procedimientos:

[1] Procedimientos de seguridad de la información (Versión 1 -25/04/2016) - MINTIC

Procedimiento De Capacitación Y Sensibilización Del Personal

La Alta Dirección debe establecer una metodología para realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones etc…

→ La Alta Dirección en cabeza de la Subdirección Administrativa debe proporcionar a todos los funcionarios un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

→ La Alta Dirección debe requerir a los funcionarios, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.

→ Todos los funcionarios de la CGA y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Procedimiento de ingreso y desvinculación del personal:

La Alta Dirección debe establecer un procedimiento que indique la manera como la entidad gestiona de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad, recepción de entregables requeridos para generar paz y salvos entre otras características.

Este procedimiento esta en cabeza de la Dirección Administrativa y financiera y va de la mano de la Subdirección Administrativa.

→ La Subdirección Administrativa y la Subdirección Operativa de la CGA deben asegurar que el abandono de la entidad por parte de los funcionarios, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso. Adicionalmente deben informar a la Dirección de Sistemas de Buen Gobierno y las TIC para eliminar el acceso a la plataforma tecnologica de la CGA.

→ La Subdirección Operativa de la CGA debe tener actualizado y verificado regularmente el inventario de los activos cargados a cada funcionario con el fin de que al momento de desvinculación la devolución de los activos de la CGA sea más sencilla.

Política De Gestión De Activos De Información

En este dominio relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad.

Procedimiento de identificación y clasificación de activos:

La Alta Dirección debe indicar la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad.

Adicionalmente se debe explicar cómo se hace una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros lugares de manera segura.

Algunos ejemplos de activos son:

✓ Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
✓
✓ Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.
✓
✓ Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.
✓

✓ Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.)

Procedimiento sobre la responsabilidad por los activos

Identificar los activos en la CGA y definir las responsabilidades para una protección adecuada.

→ La CGA es propietaria tanto de la información física como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, y debe otorgar responsabilidad a las dependencias sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

→

→ La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la CGA, son activos de la CGA y se proporcionan a los funcionarios y terceros autorizados, para cumplir con la misión de la CGA.

→ Toda la información sensible de la CGA, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Oficina Asesora de Planeación. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

→ Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

→ Los propietarios de los activos de información se encuentran sujetos a auditorías y a revisiones de cumplimiento por parte de la Oficina de Asesora de Control Interno.

→ La Dirección de Sistemas de Buen Gobierno y las TIC es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la CGA y, en consecuencia, debe asegurar su apropiada operación y administración.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la CGA.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer uso adecuado de ellos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC es responsable de preparar los

equipos computo y/o portátiles de los funcionarios y de hacer entrega de las mismas.

→ La Dirección de Sistemas de Buen Gobierno y las TIC es responsable de recibir los equipos cómputo y/o portátil y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

→ La Subdirección Operativa es responsable de recibir los equipos cómputo y/o portátil para su reasignación o disposición final.

→ Los Directores de las dependencias deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por la La Dirección de Sistemas de Buen Gobierno y las TIC.

→ Todos los funcionarios de la CGA deben utilizar los recursos tecnológicos, de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la CGA.

→ Los recursos tecnológicos provistos a funcionarios, son proporcionados con el único fin de llevar a cabo las labores misionales; por consiguiente, no deben ser utilizados para fines personales o ajenos a esta.

→ Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

→ Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la CGA.

→ En el momento de retiro, los funcionarios deben realizar la entrega de su puesto de trabajo al Jefe Inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

Procedimientos para la clasificación de la información

El objetivo es el de asegurar que se aplica un nivel de protección adecuado a la Información.

→ La CGA definirá con el apoyo de la Oficina Asesora de Planeación y de cada dependecncia los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección, ademas de identificar el acervo documental con que cuenta cada uno de los procesos.

→ Toda la información de la CGA debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por la Ley de Transparencia.

→ La CGA proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

→ La Subdirección Operativa debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.

→ La Subdirección Operativa debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

→ Los funcionarios deben acatar los lineamientos establecidos en la resolución sobre los activos de información que se encuentran publicados en la intranet: http://intranet.cga.gov.co/gestioninstitucional/Paginas/Resoluci%C3%B3n%20Activos-de-Informaci%C3%B3n.aspx para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la CGA.

→ La información física y digital de la CGA debe tener un período de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental (http://intranet.cga.gov.co/gestioninstitucional/Paginas/tablaretencion.aspx) y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

→ Los usuarios deben tener en cuenta que cuando impriman, escaneen, saquen copias: verificar que no queden documentos confidenciales para evitar su divulgación no autorizada.

→ Tanto los funcionarios deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

→ La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

Política De Control De Acceso

En este dominio relacionado con el acceso a la información y a las instalaciones de procesamiento de la información.

Para impedir el acceso no autorizado a los sistemas de información se deberán implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento

Procedimiento para ingreso seguro a los sistemas de información

El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un procedimiento donde indique como gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas, empleando métodos para cifrar la información de acceso a través de la red entre otros.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe definir procedimientos seguros de inicio de sesión, es decir, cuando sea requerido por la política de control de accesos se debera controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe realizar la gestión de contraseñas de usuario las cuales deben ser interactivos, asegurando contraseñas de calidad.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe hacer uso de herramientas de administración de sistemas. El uso de utilidades software que sean capaces de anular o evitar controles en aplicaciones y sistemas que deban estar restringidos y estrechamente controlados.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe restringuir el acceso al código fuente de las aplicaciones software.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.

→ Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la CGA deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

Procedimiento de gestión de usuarios y contraseñas

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un procedimiento, donde defina como realiza la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

→ La Dirección de Sistemas de Buen Gobierno y las TIC deben definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un procedimiento para gestionar de altas/bajas en el registro de usuarios con el objeto de habilitar la asignación de derechos de acceso.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un procedimiento para gestionar los derechos de acceso asignados a usuarios con el fin de asignar o revocar derechos de acceso para todos los sistemas y servicios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un procedimiento para gestionar los derechos de acceso con privilegios especiales el cual debe ser un proceso restringido y controlado.

→ Los propietarios de los activos deberan revisar con regularidad los derechos de acceso de los usuarios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un procedimiento para la Retirada o adaptación de los derechos de acceso para aquellos funcionarios, contratistas o usuarios de terceros que hacen uso de la información y a las instalaciones del procesamiento de información y que llegan a un estado de finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

→ Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

→ La Alta Dirección debe implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe definir una buena estrategia y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo, las cuales deben ser sensibilizadas a traves de campañas institucionales, asegurando de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado.

→ Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de

información de la CGA deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

→ Los funcionarios de la CGA no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

→ La Subdireccion Administrativa debe Solicitar a la Dirección de Sistemas de Buen Gobierno y las TIC la creación, modificación, bloqueo y eliminación de cuentas de usuario, acogiéndose al procedimiento establecidos para tal fin.

→ Los Jefes de área deben solicitar a la Dirección de Sistemas de Buen Gobierno y las TIC la definicion de perfiles de usuario para el acceso a los recursos tecnologicos de los funcionarios a su cargo.

Política seguridad física y del entorno:

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información. Se pueden generar los siguientes procedimientos:

Procedimiento de control de acceso físico

La Alta Dirección debe garantizar el control de acceso seguro a las instalaciones al personal autorizado. Se debe establecer un procedimiento que pueda incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc…

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

→ Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de La Dirección de Sistemas de Buen Gobierno y las TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su

custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe velar porque los recursos de la plataforma tecnológica de la CGA ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la CGA.

→ La Dirección Administrativa y Financiera y la Subdireccion Operativa deben proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la CGA.

→ La Dirección Administrativa y Financiera y la Subdireccion Operativa deben identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones del instituto.

→ La Dirección Administrativa y Financiera y la Subdireccion Operativa, con el acompañamiento de La Dirección de Sistemas de Buen Gobierno y las TIC, debe verificar que el cableado se encuentra protegido con el fin de disminuir las

intercepciones o daños.

→ Los ingresos y egresos de los funcionarios a las instalaciones de la CGA deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

→ Los funcionarios deben portar la escarapela que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la CGA; en caso de pérdida de la escarapela o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible a la Dirección de Sistemas de Buen Gobierno y las TIC.

→ Los funcionarios de la CGA y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

Procedimiento de protección de activos:

Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc…

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la CGA.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la CGA y configurar dichos equipos acogiendo los estándares generados.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe aislar los equipos de áreas sensibles, como la Dirección Administrativa y Financiera para proteger su acceso de los demás funcionarios de la red de la empresa.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la CGA, ya sea cuando son dados de baja o cambian de usuario.
→ La Subdirección Operativa debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la CGA, posean pólizas de seguro.

→ Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios se deben acoger las instrucciones técnicas que proporcione La Dirección de Sistemas de Buen Gobierno y las TIC.

→ Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la CGA el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de La Dirección de Sistemas de Buen Gobierno y las TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

→ La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos del instituto, solo puede ser realizado por los funcionarios de la La Dirección de Sistemas de Buen Gobierno y las TIC, o personal externo autorizado por dicha dirección.

→ Los funcionarios de la CGA deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

→ Los funcionarios de la CGA no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

→ Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

→ Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

→ En caso de pérdida o robo de un equipo de cómputo de la CGA, se debe informar de forma inmediata al Jefe inmediato para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

Procedimiento de retiro de activos

En este procedimiento debe especificarse como los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc….)

→ La Subdirección Operativa es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la

CGA.

Procedimiento de mantenimiento de equipos

Este procedimiento debe especificar como se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o si existen seguros atados a los equipos y los mantenimientos sean requisitos. Se debe especificar el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la CGA.

Seguridad de las operaciones

Este dominio busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información.

Procedimiento De Gestión De Cambios[2]

En este procedimiento la entidad deberá como realiza el control de cambios en la organización, los procesos de negocio y los sistemas de información de manera segura. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas

[2] Cobit 4.1

fundamentales.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

→ La Dirección de Sistemas de Buen Gobierno y las TIC siempre que se implantan cambios al sistema, debe actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Debe establecer un proceso de revisión para garantizar la implantación completa de los cambios.

Procedimiento De Gestión De Capacidad[3]

Se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son excasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc…

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelo apropiadas para producir un modelo de desempeño, de capacidad y de desempeño de los recursos de TI, tanto actual como pronosticado.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si

[3] Cobit 4.1

existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:
• Mantener y poner a punto el desempeño actual dentro de TI y atender temas como elasticidad, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
• Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs.

<u>Procedimiento de separación de ambientes</u>

Con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos, es necesario desarrollar un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción. Dentro de los aspectos más importantes a considerar se encuentran la implementación de un ambiente de pruebas para las aplicaciones, definición de los requerimientos para la transición entre ambientes, la compatibilidad de los desarrollos con diferentes sistemas entre otros.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe proveer la infraestructura de hardware y software necesaria para realizar la ejecución de pruebas de integración, sistema y funcionales para determinar el comportamiento de la aplicación en escenarios reales, ir probando las modificaciones que se realizan a los sistemas antes de subir dichos ajustes al ambiente de producción

<u>Procedimiento de protección contra códigos maliciosos</u>

La entidad debe indicar por medio de este procedimiento como realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.

Se debe tener en cuenta que: ¡No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables!.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la CGA y los servicios que se ejecutan en la misma.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

→ La Dirección de Sistemas de Buen Gobierno y las TIC, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

→ La Dirección de Sistemas de Buen Gobierno y las TIC, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

→ Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la La Dirección de Sistemas de Buen Gobierno y las TIC; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

→ Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en

medios de almacenamiento externos o que provienen del correo electrónico.

→ Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

→ Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que a través de ella, La Dirección de Sistemas de Buen Gobierno y las TIC se tome las medidas de control correspondientes.

Política de Seguridad De Las Comunicaciones

Este dominio busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.

Procedimiento De Aseguramiento De Servicios En La Red

Este procedimiento explica la manera en que la entidad protege la información en las redes, indicando los controles de seguridad (como se cifran los datos a través de la red por ejemplo) que se aplican para acceder a la red cableada e inalámbrica, etc… con miras a proteger la privacidad de la información que circula a través de estos medios, también se debe incluir el uso de registros (logs) que permitan realizar seguimiento a acciones sospechosas.

→ La Dirección de Sistemas de Buen Gobierno y las TIC, establecera los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la CGA.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la CGA.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma

tecnológica del instituto, acogiendo buenas prácticas de configuración segura.

→ La Dirección de Tecnología, a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el instituto en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe instalar protección entre las redes internas.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

→ La Dirección de Sistemas de Buen Gobierno y las TIC y la Oficina Asesora de Comunicaciones, deben generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

→ La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

→ Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional. El correo institucional no debe ser utilizado para actividades personales.

→ No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe proporcionar los recursos requeridos para la prestación segura del servicio de Internet de Acuerdo a los perfiles de los usuarios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe monitorear continuamente de los canales del servicio de Internet.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe realizar informes de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

→ La Dirección de Sistemas de Buen Gobierno y las TIC y La Oficina Asesora de Comunicaciones deben implementaran campañas de sensisbilización para todos los funcionarios respecto referente a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

→ Los funcionarios de la CGA deben adstenerse de descargar software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

→ No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

→ Esta prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a la misión de la CGA.

→ Esta prohibida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

→ Esta prohibido el intercambio no autorizado de información de propiedad de la CGA

entre sus funcionarios con terceros.

Procedimiento De Transferencia De Información

En este procedimiento la entidad deberá indicar como realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.

Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

→ La Subdirección Operativa debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información y que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la CGA.

→ Los propietarios de los activos de información deben velar porque la información de la CGA sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

→ Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

→ Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la CGA así como del procedimiento de intercambio de información.

→ La Oficina de Correspondencia en cabeza de la Subdirección Operativa debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

→ La Oficina de Correspondencia en cabeza de la Subdirección Operativa debe certificar

que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la CGA, y que estos permitan ejecutar rastreo de las entregas.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe ofrecer servicios o herramientas de intercambio de información seguros, y si es possible adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

→ Los terceros con quienes se intercambia información de la CGA deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad del instituto, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.

→ Los terceros con quienes se intercambia información de la CGA deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

→ Los funcionarios de la CGA no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la CGA o de sus beneficiarios.

→ No está permitido el intercambio de información sensible de la CGA por vía telefónica.

Política de Relaciones Con Los Proveedores

Este dominio está relacionado con la protección de los activos de la organización a los cuales los proveedores o terceros tienen acceso.

<u>Procedimiento para el tratamiento de la Seguridad en los Acuerdos con los Proveedores</u>

Este procedimiento debe indicar como la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan (es decir algún intermediario). Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC, la Oficina Asesora Jurídica y la Subdirección Operativa deben generar un modelo base para los Acuerdos de Niveles

de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC, la Oficina Asesora Jurídica y la Subdirección Operativa deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del instituto.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la CGA.

→ Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe verificar en el momento de la conexión y, cuando se considelre pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la CGA.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

→ Los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

→ Los Supervisores de contratos con terceros, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la

aparición de nuevos riesgos.

Política de Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información

Procedimiento Adquisición, Desarrollo Y Mantenimiento De Software

Este procedimiento deberá describir como se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad.

Se deben tener en cuenta el uso de ambientes de desarrollo, pruebas y producción para los sistemas de información.

→ Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

→ Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe solicitar a los terceros que metodologías utilizan para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

→ Los desarrolladores de los sistemas de información (internos o externos) deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

→ Los desarrolladores de los sistemas de información (internos o externos) deben

proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la CGA; dicho soporte debe contemplar tiempos de respuesta aceptables.

Procedimiento De Control Software

En este procedimiento la entidad deberá indicar como realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad, quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe contar con los sistemas de control de versiones para administrar los cambios de los sistemas de información de la CGA.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

→ La Dirección de Sistemas de Buen Gobierno y las TIC, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

→ Los desarrolladores de los sistemas de información (internos o externos) deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

→ Los desarrolladores de los sistemas de información (internos o externos) deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

→ Los desarrolladores de los sistemas de información (internos o externos) deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

→ Los desarrolladores de los sistemas de información (internos o externos) deben

asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

→ Los desarrolladores de los sistemas de información (internos o externos) deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

→ Los desarrolladores de los sistemas de información (internos o externos) deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

→ Los desarrolladores de los sistemas de información (internos o externos) deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

→ Los desarrolladores de los sistemas de información (internos o externos) deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

→ Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

→ Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

→ Los desarrolladores de los sistemas de información (internos o externos) deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

→ Los desarrolladores de los sistemas de información (internos o externos) deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

→ La Dirección de Sistemas de Buen Gobierno y las TIC protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

→ La Dirección de Sistemas de Buen Gobierno y las TIC debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

Políticas de Gestión de incidentes de seguridad de la información

Procedimiento De Gestión De Incidentes De Seguridad De La Información

Este procedimiento debe indicar como responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad.

Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes De Continuidad) dependiendo de la criticidad de la información.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

→ Los propietarios de los activos de información deben informar a la La Oficina Asesora de Control Interno, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

→ La Oficina Asesora de Control Interno debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

→ La Oficina Asesora de Control Interno debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad y Privacidad de la Información aquellos en los que se considere pertinente.

→ La Oficina de Riesgos debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.

→ La Oficina Asesora de Control Interno debe, con el apoyo con la La Dirección de Sistemas de Buen Gobierno y las TIC y la Direccion Administrativa y Financiera, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

→ El Comité de Seguridad y Privacidad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

→ Es responsabilidad de los funcionarios de la CGA y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

→ Los funcionarios de la CGA en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, deben notificarlo al superior inmediato para que se registre y se le dé el trámite necesario.

Políticas en Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio

Procedimiento De Gestión De La Continuidad De Negocio

En este procedimiento la entidad debe indicar la manera en que la entidad garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.

El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.

→ La Dirección de Sistemas de Buen Gobierno y las TIC deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

→ La Oficina Asesora de Control Interno debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

→ La Oficina Asesora de Control Interno debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

→ Los Directivos de cada una de las dependencias de la CGA deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

Bibliografía

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). *Modelo de Seguridad y Privacidad de la Información - Seguridad y Privacidad dela Información – Modelo - – Versión 3.0.2*.

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). *Elaboración de la política general de seguridad y privacidad de la Información. – Seguridad y Privacidad de la Información – Guía No. 2 - Versión 1.*

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). *Procedimientos De Seguridad De La Información. – Seguridad y Privacidad dela Información – Guía No. 3 - Versión 1.*

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). *Controles de Seguridad y Privacidad de la Información. - Seguridad y Privacidad dela Información – Guía No. 8 - Versión 3.0.1.*

ICONTEC, (2006). *Norma Técnica Colombiana NTC-ISO/IEC 27001. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos*.

Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, (2013). *ISO/IEC 27002:2013. Mejores prácticas en la gestión de la seguridad de la Información*.

IT Governance Institute, (2007). *Marco de Trabajo COBIT 4.1. Estándares internacionales para la dirección y control de la tecnología de la Información.*

Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior –ICETEX. (2014). *Manual de Políticas de Seguridad de la Información* – Recuperado el 1 de septiembre de 2016, de

https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf ISO 27002. Recuperado el 1 de septiembre de 2016, de http://www.iso27000.es/iso27002.htm

RESOLUCIÓN

ARTICULO SEGUNDO: El Director Técnico, es responsable de dar a conocer a todos los funcionarios de su área de gestión el Proceso y de supervisar periódicamente su adecuada aplicación.

ARTÍCULO TERCERO: Los formatos a utilizar en la ejecución del Proceso no harán parte de éste. Para conocimiento y aplicación de los funcionarios que intervienen en el Proceso, dichos formatos estarán dispuestos en la Intranet "Sistema de Gestión Institucional/Formatos". Para la modificación de los formatos, se requerirá de Vº.Bº del

Jefe de la Oficina Asesora de Planeación y desde esta Área de Gestión se realizará el control sobre la actualización de los mismos

ARTICULO CUARTO: La presente Resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE, PUBLÍQUESE Y .CÚMPLASE

SERGIO ZULUAGA PEÑA
Contralor General de Antioquia

P/E: Nancy Stella García Ospina, Profesional Universitario, Diego Alonso García Ospina, Profesional Especializado, Patricia Carvajal Vargas, Contralora auxiliar Planeación
R/: Luis Carmelo Cataño, Director Técnico, Juan Carlos Peláez Serna, Jefe Oficina Asesora de Comunicaciones,
A/: Sergio Zuluaga Peña, Contralor General de Antioquia.