POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA MAYOR DE BOGOTÁ D.C. GOBIERNO SEGURIDAD Y CONVIVENCIA Instituto Distrital de la Participación y Acción Comunal	**INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL**		
SISTEMA INTEGRADO DE GESTIÓN			
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			
CÓDIGO:	IDPAC-GTI-OT-04	**VERSIÓN**	01
ELABORÓ	**REVISÓ**	**APROBÓ**	
Oscar Gallo Bonilla	**Veronica Basto Mendez**	**Antonio Hernandez Llamas**	
Contratista	Jefe Oficina Asesora de Planeación	Director General	
Cristian David Castro Sanchez	**Camilo Alejandro Posada**	**Hugo Alberto Carrillo Gomez**	
Contratista	Jefe Oficina Asesora Jurídica	Secretario General	
FECHA	**FECHA**	**FECHA**	

REGISTRO DE MODIFICACIONES		
VERSIÓN	**FECHA**	**ÍTEM MODIFICADO – DESCRIPCIÓN**
01	22/08/2017	Versión Inicial

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Bogotá Distrito Capital
Instituto Distrital de la Participación y la Acción Comunal - IDPAC
Septiembre de 2017

CONTENIDO

1. INTRODUCCIÓN

La seguridad informática dispone de lineamientos técnicos y legales para garantizar la confidencialidad, integridad y disponibilidad de la información del Instituto Distrital de la Participación y la Acción Comunal - IDPAC, incluye los dominios sugeridos por la norma técnica internacional ISO 27002:2013, que responden a las necesidades de la Entidad y que contribuyan al alcance de las metas institucionales.

Esta política debe ser aplicada por todos los funcionarios, contratistas, proveedores, y todo personal externo que utilice los servicios de tecnologías de la información que ofrece la Entidad; deben conocer y aceptar el reglamento vigente para su uso y el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier acción de amenaza que afecte la seguridad de la información de la Entidad.

2. OBJETIVO

El objetivo del presente documento es establecer las políticas en seguridad de la información del Instituto Distrital de la Participación y la Acción Comunal, con el fin de regular la gestión de la seguridad de la información, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

3. ALCANCE

La presente Política de Seguridad de la Información se establece en cumplimiento de las disposiciones legales vigentes, con el objeto de implementar una adecuada gestión de la seguridad sobre los activos de información definidos por la Entidad, debiendo ser conocida y de obligatorio cumplimiento por parte de funcionarios, contratistas y terceros que acceden al uso de las plataformas y servicios tecnológicos que disponga la Entidad.

4. MARCO LEGAL

El Instituto Distrital de la Participación y la Acción Comunal acoge las normas vigentes de seguridad de información, protección de datos personales y directrices de ciberseguridad a nivel nacional, aplicando las prácticas y estándares recomendados para su cumplimiento.

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Directiva	05	Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital	2005		X	

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Resolución	305	Por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre	2008		X	
Ley	1273	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	2009	X		
Decreto	235, Art.1-4	Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones pública	2010	X		
Ley	1581	Por la cual se dictan disposiciones generales para la protección de datos personales.	2012	X		
Decreto	1377	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	2013	X		

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Ley	1712	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.	2014	X		
Decreto	2573	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones	2014	X		
Decreto	1074	"Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo."	2014	X		
Decreto	415	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	2016			
Directiva	03	Creación equipo de trabajo de seguridad de la información adscrito a la Dirección General.	2016			X
Resolución	116	Por la cual se crea el Comité de Seguridad de la Información (CSI) del Instituto de la Participación y la Acción Comunal	2017			X

4.1. Documentos de referencia

Tipo Documento	Título del documento	Código	Origen	
			Extern	Intern
Norma Técnica Distrital	Norma Técnica Distrital SIG 001:2011. Capítulo 6 Seguimiento y Monitoreo del Desempeño de la Seguridad de la Información.	SIG 001:2011	X	
Conpes 3854	Política Nacional De Seguridad Digital		X	
Norma Técnica Internacional ISO 27001, 27002, 27005	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información.	ISO 27001, 27002, 27005 :2013	X	

5. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de exposición al riesgo.

Confidencialidad: propiedad que determina que la reserva de la información, es decir que no esté disponible ni sea revelada a individuos, entidades, terceros indeterminados o procesos no autorizados.

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.

Criptografía: Técnica de codificar u ocultar r mensjaes o textos como claves o información que no debe ser vista salvo por la persona a quien está dirigida.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de *una entidad autorizada.*

Etiquetar Información: Referenciar registros de información acuerdo a un inventario y clasificación de la información.

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las actividades de la entidad y amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Plan de Contingencia: Procedimientos alternativos de una Entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

Plan de Pruebas de Recuperación: Pruebas de recuperación de copias de respaldo programadas con el fin de verificar la consistencia e integridad de las copias de respaldo.

Plataforma Tecnológica: Una plataforma tecnológica es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos para la realización de las tareas de los usuarios

Política: Instrucciones mandatorias que indican la intención y la directriz de la alta gerencia respecto a la operación de la Entidad.

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.

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Sistema de gestión de la 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 del riesgo y de mejora *continua.*

Software: Conjunto de programas, aplicaciones y rutinas que se ejecutan en un computador.

Software utilitario: Software que está diseñado para realizar una tarea determinada o especifica

TI: se refiere a tecnologías de la información

TIC: se refiere a tecnologías de la información y comunicaciones

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.

6. DOMINIOS POLÍTICAS DE SEGURIDAD

6.1. Políticas de seguridad de la información

Objetivo: Determinar las directrices para la Entidad en lo relacionado con Seguridad de la Información.

El Comité de Seguridad de la Información será el responsable de la definición, elaboración, actualización, implementación, monitoreo y seguimiento de la Política de Seguridad de la Información, asegurando así los recursos adecuados y promoviendo una cultura activa de seguridad de la información en la Entidad.

Los (as) funcionarios(as), contratistas y/o terceros que realicen labores en o para la Instituto Distrital de la Participación y la Acción Comunal, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

Los directores y jefes de área serán los responsables de hacer cumplir las políticas y directrices de seguridad de la información establecidas en la Entidad.

Las auditorias y seguimientos a los sistemas de información se realizarán de manera preventiva por los funcionarios o contratistas designados por el Secretario General.

Los usuarios de los activos de información deberán notificar al Comité de Seguridad de la Información, las inconsistencias, anomalías e incidentes de seguridad, tales como:

- Eventos adversos o anormales en computadores, sistemas de información asignados, redes de datos, equipos de comunicación.
- Cuando exista sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin autorización.

El Comité de Seguridad de la Información revisará anualmente la presente Política, a efectos de mantenerla actualizada. Así mismo efectuará toda modificación que sea

necesaria en función a posibles cambios que puedan afectar su definición, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios estructurales de la Entidad, entre otros.

Cualquier usuario de los servicios tecnológicos de la entidad puede identificar la necesidad de modificar la Política de Seguridad de la Información. Dichas inquietudes y sugerencias deben ser comunicadas al Comité de Seguridad de la Información, responsable por el mantenimiento de la misma.

6.2. Organización de la seguridad de la información

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la Entidad.

Directrices:

Esta política debe ser aplica por todos los servidores públicos, contratistas y particulares que tengan acceso y uso de los activos de información de la entidad.

El Comité de la Seguridad de la Información del Instituto Distrital de la Participación y Acción Comunal fue establecido mediante la Resolución 116 del 07 de Abril de 2017, siendo la máxima Autoridad de Seguridad de la Información y por tanto el responsable de generar, modificar y aprobar las políticas específicas de seguridad de la información aplicables al interior de la Entidad, así como los procesos, procedimientos, controles y directrices de seguridad de la información para el adecuado uso y administración de los activos de información.

6.2.1. Asignación de responsabilidades para la seguridad de la información

Las responsabilidades de seguridad de la información están definidas y asignadas de acuerdo a la clasificación dada a la información.

El uso de activos de la información serán autorizados por los directores o Jefes de áreas responsables de las dependencias involucradas, considerando su propósito y uso, conjuntamente con los Responsables de la Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas, directrices y requerimientos de seguridad pertinentes.

6.2.2. Segregación de las tareas

La responsabilidad sobre los Activos de la información deberá estar en cabeza del responsable de la información definido dentro de la Entidad, para evitar conflicto en cuanto a responsabilidades.

6.2.3. Contacto con grupos de interés especial

La Entidad podrá compartir experiencias y cooperar en materia de seguridad, con entidades territoriales y nacionales del Estado, previa firma de un convenio o acuerdo de confidencialidad de los temas de seguridad tratados.

Se mantendrán los contactos apropiados con los grupos de interés especial como la Alta Consejeria Distrital de TIC, Comisión Distrital de Sistemas, Ministerio de TIC, Policía y demás entes de seguridad especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el evento en que se presente un incidente de seguridad de la información.

6.2.4. Uso de dispositivos móviles y seguridad de la información

El uso de los equipos de cómputo fuera de las instalaciones de la Entidad, únicamente se permitirá a usuarios autorizados por la Secretaria General, previa solicitud de la dependencia respectiva, y éstos se protegerán mediante el uso de controles tecnológicos y administrativos.

6.2.5. Teletrabajo

Los funcionarios y contratistas de la Entidad autorizados por la Secretaria General que requieran tener acceso y uso de activos de la información de la Entidad desde redes externas, podrán acceder remotamente mediante un proceso de autenticación y uso de conexiones seguras, lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

6.3. Seguridad de los recursos humanos

Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades e idoneidad en los roles para las funciones que se consideran.

En los procesos de inducción y reinducción que se adelanten, se informará a funcionarios y contratistas de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

Los usuarios son responsables de entender y seguir los procedimientos y directrices establecidos para la utilización de los activos de información de la Entidad. Así mismo, son responsables de informarse y seguir las directivas comunicadas por correo electrónico u otros medios de información implementados o a implementarse.

El Responsable del Área Jurídica participará en la estructuración del Compromiso de Reserva y Confidencialidad de la Información, a firmar por los funcionarios, contratistas y terceros que desarrollen funciones en la Entidad.

Se prohíbe a los usuarios la realización de pruebas de seguridad o de realizar cambios en los activos de información para eliminar o minimizar anomalías de seguridad. El Comité de seguridad de la información es el encargado de asignar los recursos para la realización de pruebas para detectar, verificar o eliminar una supuesta debilidad o falla de seguridad.

6.3.1. Antes de la contratación

Investigación de antecedentes

Se realizará la verificación de antecedentes judiciales, disciplinarios, fiscales y seguimiento a la hoja de vida de todos los candidatos a servidores públicos y de las personas naturales que aspiren a suscribir contratos con la Entidad de conformidad con el reglamento interno de la Entidad y las leyes y regulaciones del estado colombiano.

Términos y condiciones de contratación

Los Funcionarios y contratistas deben aceptar las políticas, directrices y procedimientos de seguridad de la información que deben aplicar. Para ello se deben establecer acuerdos de confidencialidad, cláusulas u obligaciones contractuales, funciones y obligaciones, dependiendo de la modalidad de contratación.

6.3.2. Durante la contratación

Concientización, educación y formación en la seguridad de la información

Se realizará sensibilización en forma periódica a los funcionarios y contratistas de la Entidad, sobre las políticas de seguridad de la información que se encuentren vigentes.

Proceso disciplinario

Los funcionarios y contratistas deben cooperar con los esfuerzos por proteger los activos de información aplicando las directrices y controles de seguridad implementados.

Se solicitará proceso disciplinario formal contra los funcionarios y contratistas que comentan o hayan cometido violación contra la seguridad de la información.

6.3.3. Terminación o cambio de empleo

Devolución de activos

Los funcionarios o contratistas deberán devolver los activos de información a su cargo y cuentas de usuario, por motivo de retiro definitivo o temporal, cambio de puesto de trabajo, licencias o vacaciones, suspensión y/o finalización del contrato.

Retirada de los derechos de acceso

La vigencia de los derechos de acceso a la infraestructura de tecnologías de la información, debe estar estrechamente relacionados con la terminación de la relación laboral y/o contractual del servidor público y/o cambio del rol del servidor público en la Entidad.

6.4. Gestión de activos de la Información

Objetivo: Identificar los activos de la Entidad y definir las responsabilidades de protección adecuados.

Los propietarios responsables de los Activos de Información, tienen la responsabilidad de colaborar en la vigilancia del cumplimiento de la Política de Seguridad de la Información dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios en su uso.

El Comité de la Seguridad de la información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

6.4.1. Inventario de activos de la Información

Los activos relacionados con el tratamiento de la información, la información propiamente dicha y las instalaciones de procesamiento de información deben ser identificados y clasificados bajo un inventario de activos de la Entidad.

6.4.2. Propiedad de los activos de Información

Los activos mantenidos en el inventario son de propiedad del Instituto Distrital de la Participación y Acción Comunal.

6.4.3. Uso aceptable de los activos de Información

Las normas para el uso aceptable de la información y de los activos asociados a la información y las instalaciones de procesamiento de información están definidas en documentos de directrices y controles del Subsistema de Gestión de la Seguridad de la Información.

6.4.4. Devolución de los activos de Información

Los funcionarios y contratistas deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.

6.4.5. Clasificación de la información

Los activos de información se clasificarán de acuerdo a los principios de fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad, conforme a la evaluación que se realice sobre las características de su valor relativo, su privacidad, sensibilidad, el nivel de riesgo a que está expuesta y/o requerimientos legales de retención.

6.4.6. Categorización de los activos de información según la confidencialidad

Principio que se le debe dar a la existencia de información que puede o debe ser divulgada o no. Dando alcance a los criterios de clasificación de la información definidos en la Ley 1712 de 2014, la Entidad aplicará los siguientes criterios a los activos de información: *Pública*, *Reservada*, *Privada o Confidencial*, *Semi-privada o Interna.*

6.4.7. Almacenamiento de Información.

Los equipos de cómputo que almacenen información reservada, privada o confidencial deben estar protegidos con mecanismos de seguridad para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información allí almacenada. Así mismo si son reasignados a usuarios diferentes, se debe borrar la información del disco duro de forma segura, de acuerdo a los lineamientos dados por el responsable de seguridad de la información.

6.4.8. Impresión de información.

Los documentos que se impriman y/o digitalicen en equipos de la Entidad deben ser de carácter institucional.

La información clasificada reservada, privada o confidencial debe ser enviada a la impresora y recogida inmediatamente, evitando que personal no autorizado tenga acceso a ésta.

6.4.9. Divulgación de información a terceros.

Los funcionarios y contratistas no deben divulgar información reservada, privada o confidencial a terceros sin la autorización de los responsables de la información y la firma de un acuerdo de confidencialidad

6.4.10. Etiquetado y manipulado de la información

Los procedimientos para el etiquetado de la información serán aplicados de acuerdo con el esquema de clasificación de la información aprobada por la entidad, lo anterior teniendo en cuenta las Tablas de Retención Documental aprobadas para las diferentes áreas.

6.4.11. Gestión de soportes extraíbles

La gestión de medios extraíbles se realizará de acuerdo con el esquema de clasificación adoptado por la entidad. Los equipos de cómputo que tienen autorizado el uso de puertos para conexión USB y unidades reproductoras de CD/DVD, deben cumplir los siguientes requisitos:

- Tener habilitado el escaneo automático de virus.
- Tener configurada en la herramienta de antivirus institucional, el bloqueo de la reproducción automática de archivos ejecutables

6.4.12. Eliminación de soportes.

La información será eliminada de los medios de comunicación de forma segura cuando ya no sea necesaria, utilizando procedimientos formales.

6.4.13. Soportes físicos en tránsito

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte. Se debe implementar la utilización de protocolos de seguridad para la encriptación de las claves y documentos con información reservada.

6.5. Control de acceso a la Información

Objetivo: Limitar y controlar el acceso y uso de los activos de información a funcionarios y contratistas y terceros que estén vinculados a la Entidad.

La Entidad establece entornos con controles de acceso que aseguran el perímetro de oficinas, recintos, como en entornos abiertos para evitar el acceso no autorizado a ellos, controlando las amenazas físicas externas y velando por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y la preservación de sus activos de información.

Así mismo, se exige a los proveedores de servicios de tecnología, el cumplimiento de la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con que éste debe contar.

Los funcionarios y contratistas responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las medidas de seguridad definidas.

Los directores y Jefes de área como responsables de la información, colaborarán en la definición de los controles de acceso a los activos de información, y ayudarán a monitorear que los activos de información sean accedidos únicamente por los usuarios autorizados.

6.5.1. Gestión de acceso de usuario.

Registro de usuario.

Se asignará una cuenta o identificador de usuario mediante la cual se podrá realizar el registro de acceso a los activos de información. La cuenta de usuario debe ser única.

El nivel de acceso otorgado debe ser el adecuado para el propósito de la función del usuario y debe ser coherente con la Política de Seguridad de la Entidad, por ejemplo, que no comprometa la separación de tareas.

Se realizará revisiones periódicas con el objeto de cancelar cuentas de usuario redundantes o inactivas.

El acceso a los Activos de Información de la Entidad, debe ser gestionado mediante un procedimiento formal de creación, modificación y eliminación de cuentas de usuario.

Únicamente el responsable de la información, puede autorizar la creación, modificación y eliminación de cuenta de usuario.

Gestión de derechos o privilegios.

Se limitará y controlará el acceso y uso de activos de información mediante la asignación de permisos o privilegios a las cuentas de usuario, debido a que el acceso y uso inadecuado de la información o cualquier recurso informático de la Entidad genera un impacto negativo en la administración de la información, y es frecuentemente, un factor importante que contribuye a fallas y alteraciones de los sistemas de información a los que se ha accedido ilegalmente o inadecuadamente.

Gestión de contraseñas de usuario.

Se garantizará que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema.

Se configurarán los sistemas de información de tal manera que las contraseñas sean fuertes, no repetibles en un periodo de tiempo o *n* cambios anteriores, bloqueo de cuentas después de "*n"* intentos fallidos, solicitud de cambio de tiempo después de cumplido un periodo de tiempo.

Revisión de los derechos de acceso de usuario

Los responsables de activos deben revisar los derechos y autorización de acceso y privilegios de los usuarios de acceso de los usuarios a intervalos regulares. Cualquier desviación será tratada como un incidente en seguridad de la información. Los responsables deben dejar trazabilidad del ejercicio de ésta actividad, las que serán objeto de revisiones de parte de la Entidad.

Gestión de derechos de acceso con privilegios especiales

El uso de las claves de usuarios administradores de plataformas tecnólogicas, tienen un control especial, estas deben ser cambiar obligatoriamente cada mes, y se deben entregar en sobre cerrado al responsable del Activo de Información y clasificarse como información reservada y confidencial.

Retirada o adaptación de los derechos de acceso

Los privilegios otorgados a las cuentas de usuario de funcionarios y contratistas de la Entidad serán retirados en el momento de retiro de su empleo y/o terminación de contrato.

6.5.2. Responsabilidades de usuario.

Uso de contraseñas

Los funcionarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos de la Entidad, mediante la utilización de contraseñas confidenciales y de uso personal.

Equipo de usuario desatendido

Los usuarios deben concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un protector de pantalla protegido por contraseña.

Los usuarios deben proteger los computadores asignados contra usos no autorizados mediante un bloqueo por contraseña de acceso cuando no se utilizan.

Política de puesto de trabajo despejado y pantalla limpia.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en áreas de tratamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

6.5.3. Control de acceso a la red.

Política de uso de los servicios en red.

El correo electrónico es un medio de comunicación institucional; el uso de internet es estrictamente de carácter institucional, esos servicios se monitorearán periódicamente o por solicitud de los órganos de control para verificar su adecuada utilización.

Ningún equipo de cómputo o de comunicaciones que no sea de propiedad de la Entidad debe ser conectado a la red institucional. En caso de ser necesario el acceso a internet para este tipo de equipos se ha dispuesto una red WiFi de uso exclusivo para visitantes y ciudadanos.

Solo se instalarán computadores personales u otros dispositivos con la autorización de la Secretaria General y previo análisis y verificación de la situación de vulnerabilidad de la Entidad.

Los encargados del soporte técnico deben desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

La Secretaria General es responsable del monitoreo, diseño de mecanismos e implementación de protocolos de seguridad y reporte de incidentes en el uso de internet y red wifi.

La Entidad considerará el abuso en la utilización de recursos informáticos como una falta disciplinaria.

Autenticación de usuario para conexiones externas.

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Entidad. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación previa autorización de acceso de la Secretaria General. El Responsable de Seguridad Informática, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso

6.5.4. Control de acceso al sistema operativo.

Identificación y autenticación de usuario.

Todos los usuarios tendrán una cuenta de usuario (identificador) única de red para su uso personal exclusivo, de manera que las actividades realizadas por el usuario sean trazables y no puedan ser repudiadas.

Sistema de gestión de contraseñas.

Se revisará el sistema de administración de contraseñas de la Entidad para verificar que se cumplan las directrices de la gestión y uso de Contraseñas de usuario.

El sistema permitirá que los usuarios seleccionen y cambien sus propias contraseñas cuando lo deseen o luego de cumplido el plazo mínimo de mantenimiento de las mismas.

Uso de los recursos del sistema.

Se limitará y se controlará el uso de software utilitario a usuarios autorizados, diferentes a software de aplicaciones, para evitar que se pase por alto los controles de sistemas y aplicaciones. Se removerá todo software utilitario que no se requiera o no esté autorizado por la Secretaria General para la administración y operación de los servicios de tecnología.

Desconexión automática de sesión.

Se deberá implementar la desconexión de computadores por tiempo de inactividad, que bloquee el equipo y evite el acceso no autorizado, sin que se cierren las sesiones de aplicación o de red.

Limitación del tiempo de conexión.

Las aplicaciones proveerán un mecanismo de desconexión automática por tiempo de inactividad en el uso de la aplicación, que podrá ser independiente del tiempo de inactividad de la estación de trabajo o computador.

6.5.5. Control de acceso a las aplicaciones y a la información.

Restricción del acceso a la información.

Todas las aplicaciones y bases de datos que se utilicen deben tener cuentas de usuario para su acceso y establecer perfiles de usuario para acceder a la información.

Acceso a sistemas de información y aplicaciones

El acceso a la información en producción de la Entidad debe hacerse únicamente a través de los aplicativos y sistemas autorizados. En ningún caso la información puede ser accedida directamente.

Si entes externos tienen acceso a información crítica de la Entidad se deben suscribir acuerdos de confidencialidad para la salvaguarda de la información.

Aislamiento de sistemas sensibles.

Según las necesidades de la Entidad, se aislarán los computadores donde se procese la nómina de la entidad, se lleven procesos disciplinarios, evaluaciones para la selección de contratistas o donde se autoricen o se realicen pagos en línea, asi como la información de carácter sensible perteneciente a las Juntas de Acción Comunal (JAC).

Control de acceso al código fuente de los programas

El acceso a los archivos de código fuente de las aplicaciones de software es limitado. Solamente el personal autorizado por la Secretaria General tendrá acceso a esta información y harán uso de la misma. Se debe controlar y supervisar el acceso y uso a los archivos de código fuente de las aplicaciones de software.

6.6. Criptografía

Objetivo: Asegurar el acceso y uso adecuado y efectivo de la información para proteger la confidencialidad, autenticidad y/o integridad de la información.

La política sobre uso, protección y duración de las claves criptográficas se realiza a través del directorio activo durante todo su ciclo de vida.

Se deben utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.

- Para la transmisión de información clasificada, fuera del ámbito de la Entidad.

- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el responsable de la Información y el responsable de Seguridad Informática.

6.7. Seguridad física y del entorno

Objetivo: Evitar el acceso físico no autorizado, daños e interferencia para la información de la Entidad y las instalaciones de procesamiento de información.

Contar con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios.

Mantener la seguridad en los momentos de mantenimiento, cuando la información o los equipos que la contienen deben salir de la Entidad o cuando se deben eliminar o dar de baja, para lo cual deben existir procedimientos especiales.

6.7.1. Áreas seguras

Perímetro de seguridad física.

Todas las áreas o dependencias administrativas y operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en red (planos de cableado estructurado) los cuales deben estar compendiados y disponibles en su respectivo cuarto de equipos y comunicaciones. En

estos planos se deben identificar cuáles son las áreas seguras, con acceso restringido a personal no autorizado.

Controles físicos de entrada.

Todos los funcionarios y contratistas deberán portar el carnet en lugar visible, permitiendo con esto una mejor identificación y control de las personas que ingresan a las áreas de cómputo y/o de archivo documental restringidas.

Seguridad de oficinas, despachos e instalaciones

Todas las oficinas donde se procese y almacene información deben tener acceso restringido a personal no autorizado.

Las puertas y ventanas de las áreas seguras deben permanecer cerradas cuando no haya vigilancia e inspeccionar periódicamente las áreas protegidas desocupadas. Se agregará protección externa a las ventanas que presenten riesgos especiales.

Protección contra las amenazas externas y de origen ambiental.

La Secretaria General debe garantizar la adopción de los controles necesarios para asegurar que los suministros de electricidad, así, como las redes de comunicaciones se encuentran protegidos.

Los equipos de cómputo de la Entidad se instalarán en lugares adecuados, lejos de polvo y tráfico de personas y garantizando las condiciones para su adecuado funcionamiento.

La Secretaría General debe monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.

La Entidad mantendrá póliza de seguros de los recursos informáticos en funcionamiento. Se debe incluir en la póliza colectiva de seguros el riesgo ante posibles pérdidas de información, por daños irrecuperables en los medios de información.

Trabajo en áreas seguras.

Son áreas seguras las áreas de archivo documental, sitio donde se ubican equipos de cómputo de tratamiento de información sensible y/o critica, las áreas de informática y sistemas de la Entidad, como centro de datos internos o externos, centros de cableados, cuartos de Unidades de poder no interrumpida – UPS, laboratorio de soporte.

En las áreas seguras se debe incrementar la seguridad, se establecen directrices y controles para asegurar la seguridad sobre los activos de información que estén estos sitios.

Áreas de acceso público, de carga y descarga.

En áreas de atención directa al público, zonas de entrega y carga y puntos en los que las personas no autorizadas puedan entrar, los equipos de cómputo deberán estar aislados o se instalarán de manera que el público no tenga acceso directo al equipo.

6.7.2. Seguridad de los equipos.

Emplazamiento y protección de equipos.

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.

Cada usuario es responsable del cuidado del hardware y software suministrado por la entidad. En consecuencia, cada usuario responderá por los daños y perjuicios técnicos y legales ocasionados por su mala utilización. La detección de este uso indebido podrá ocasionar la inhabilitación temporal o definitiva del activo de información para el usuario responsable.

Los computadores se instalarán sobre escritorios o muebles estables o especialmente diseñados para ello, alejados de la luz del sol y de las ventanas abiertas.

Seguridad del cableado.

El cableado de energía eléctrica y de comunicaciones, deberán cumplir con los estándares vigentes y resguardados del paso de personas o máquinas y libres de cualquier interferencia eléctrica o magnética.

Cuando en las instalaciones eléctricas se alimenten elevadores, aspiradoras, cafeteras, motores y otros equipos, se deberá tener un circuito independiente según los estándares que rigen la materia

Mantenimiento de los equipos.

Con el fin de garantizar un correcto funcionamiento y disponibilidad de los equipos de cómputo, se debe realizar mantenimiento preventivo y correctivo, mediante la contratación de firmas especializadas que presten este tipo de servicio o en su defecto por el personal soporte técnico de la Entidad, quienes deben tener a su disposición las herramientas necesarias para efectuar dichos mantenimientos.

- Mantenimiento Preventivo y correctivo

El mantenimiento preventivo de equipos de cómputo se realizará según plan, por lo menos cada seis meses.

La Secretaria General es la responsable de coordinar la reparación de los equipos de cómputo de propiedad de la Entidad. Las reparaciones o ampliaciones de los equipos no pueden ser hechas o contratadas por el usuario.

La Secretaria General a través del personal de soporte o del proveedor del servicio de mantenimiento mantendrá una hoja de vida de cada equipo, que contemple las revisiones efectuadas, cambio de piezas, modificaciones realizadas, fecha de vencimiento de la garantía, contrato de mantenimiento vigente y ubicación actual.

Esta prohibido que los técnicos de sistemas de la Entidad realicen el mantenimiento preventivo o correctivo de equipos que no son propiedad de la Entidad dentro de las instalaciones de la entidad y en horas laborales.

- Solicitud de Mantenimiento

Para el mantenimiento correctivo, o solicitud de mantenimiento preventivo el usuario del equipo de cómputo, deberá realizar solicitud al área de soporte técnico de Sistemas.

La Secretaria General debe definir los acuerdos de niveles de servicio operativo que se deben cumplir para la atención y solución del requerimiento de los servicios de mantenimiento.

Seguridad de los equipos fuera de las instalaciones.

El uso del equipo destinado al procesamiento de información fuera de las instalaciones de la Entidad, será autorizado por la Secretaria General. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el responsable de la misma.

Mantener pólizas de seguros con una adecuada cobertura para proteger los recursos informáticos fuera de las instalaciones de la Entidad.

Retirada de materiales propiedad de la Entidad

Ningún activo de información será retirados de una sede de la Entidad sin autorización formal. El personal de vigilancia será el encargado de controlar la salida del recurso con la debida autorización.

Reutilización o eliminación segura de dispositivos de almacenamiento

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Equipo informático de usuario desatendido

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada.

6.8. Seguridad de las operaciones

Objetivo: Asegurar operaciones correctas y seguras en el procesamiento de información.

La Secretaria General tendrá la responsabilidad de la definición, documentación, verificación de los procesos, procedimientos e instructivos de las actividades relacionadas con la gestión de Tecnologías de la Información.

La Secretaria General encargada de la operación y administración de la plataforma tecnológica que apoya los procesos de la Entidad, asignará funciones específicas a sus funcionarios y/o contratistas, quienes actuarán como responsables de garantizar la adecuada operación y administración de dicha plataforma, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de dichas actividades.

6.8.1. Responsabilidades y Procedimientos de operación

Documentación de Procedimientos de operación

Se debe proveer a sus funcionarios de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información (comunicaciones y servicios como correo, intranet, WEB) así como todos los componentes de la plataforma tecnológica de la entidad.

Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de la Entidad.

Gestión de cambios

La Secretaria General establecerá, coordinará y controlará los cambios realizados en los activos de información, asegurando que los cambios efectuados sobre la plataforma tecnológica, serán debidamente autorizados por las áreas correspondientes.

Los responsables de los activos de información deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

El Cómite de Seguridad de la Información controlará que los cambios en los componentes de producción y de comunicaciones no afecten la seguridad de los mismos, ni de la información que soportan. La Secretaria General evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se debe garantizar que todo cambio realizado sobre la plataforma tecnológica de la Entidad, quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.

Mientras se establece que el cambio está en producción de manera satisfactoria se mantendrá un seguimiento que contenga toda la información relevante de cada cambio implementado.

Segregación de tareas

La asignación de tareas de operación y apoyo a la gestión estarán separadas del seguimiento y verificación de seguridad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas. Por ejemplo:

- Las funciones operativas y de soporte del proceso de Gestión de Tecnologías de la Información y las funciones de seguridad de la información, en ningún caso serán prestadas o ejecutadas por el mismo funcionario o contratista.
- El desarrollador de aplicaciones no podrá ser administrador de bases de datos en producción, ni administrador de aplicaciones o sistemas de información.
- Los funcionarios o contratistas con funciones operativas o soporte en plataformas tecnologicas no tendrán a su cargo funciones de auditoria de seguridad de la información o de control interno.
- El interventor de un contrato no debe ser el mismo que efectúa el pago.

Separación de entornos de desarrollo, prueba y producción

Los ambientes de desarrollo, las pruebas y producción deberán estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo. Se debe garantizar los recursos necesarios que permitan la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios que ejecutan dichas labores.

6.8.2. Gestión de la provisión de servicios por terceros.

Provisión de servicios.

Al contratar con terceros, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes consideraciones:

- Identificar las aplicaciones sensibles o críticas que convenga retener en el Entidad.
- Obtener la aprobación de quienes son o serán los responsables de aplicaciones y/o servicios específicos.
- Especificar las normas de seguridad y el proceso de medición del cumplimiento.
- Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.

- Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Supervisión y revisión de los servicios prestados por terceros.

Se deberá establecer con los proveedores Acuerdos de Niveles de Servicio y las respectivas penalizaciones en caso de incumplimiento en la prestación de servicios. Las penalizaciones por incumplimiento de los niveles de servicio, son diferentes a las multas estipuladas por incumplimiento del contrato. Se deberá garantizar el monitoreo de los acuerdos de niveles de servicio establecidos.

6.8.3. Planificación y aceptación del sistema.

Gestión de capacidades.

La Secretaria General efectuará el monitoreo de las necesidades de capacidad de los sistemas en producción y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además de los nuevos requerimientos de tecnología informática, las tendencias actuales y proyectadas en el procesamiento de la información. Así mismo, informará los eventos que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento.

Aceptación del sistema.

La Secretaria General y el Responsable de Seguridad Informática definirán los criterios de aprobación de los nuevos sistemas de información, actualizaciones y nuevas versiones.

6.8.4. Protección contra el código malicioso y descargable.

Controles contra el código malicioso.

Se implementará una plataforma de antivirus debidamente licenciada con la funcionalidad de actualización permanente de sus bases de virus y mediante el cual todo medio de almacenamiento, como disquete, cinta, discos duros removibles, dispositivos con conexión USB, Discos compactos, que ingrese a la entidad debe ser revisado y/o vacunado, como media previa antes de su uso.

En caso de necesitar la instalación de algún software adicional de protección y detección de código malicioso, se debe contar con la autorización de la Secretaria General.

Controles contra el código descargado por usuarios.

Se implementarán políticas de descarga de aplicaciones software que eviten que usuarios no autorizados puedan descargar e instalar software.

6.8.5. Copias de seguridad.

Se establecen directrices y controles para administrar las copias de seguridad que aseguren la disponibilidad y confidencialidad de la de las bases de datos que contienen la información institucional, configuraciones y parámetros de aplicaciones de software, sistemas de información y demás servicios, esta tarea debe realizarse diariamente y de forma automática.

Se debe contar con procedimientos para realizar las copias de respaldo y su restauración para garantizar su integridad y usabilidad en caso de ser requerido.

Se realizarán pruebas periódicas de recuperación de la información respaldada y documentar sus resultados, con el fin de garantizar la integridad de la información resguardada.

6.8.6. Manipulación de los soportes

Gestión de soportes extraíbles.

La Secretaria General con la asistencia del Responsable de Seguridad de la información autorizaran:

Uso de medios informáticos removibles, como cintas, discos, dispositivos de almacenamiento USB e informes impresos.

Eliminar de forma segura los contenidos (Documentos en papel, audios, videos, fotografías, papel carbón, Informes o reportes, Cintas de impresora de un solo uso, cintas magnéticas, discos o casetes removibles, medios de almacenamiento, listados de activos de información, datos de prueba y documentación del sistema.), si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Entidad.

Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Procedimientos de manipulación de la información.

Se definirán procedimientos para el manejo y almacenamiento de la información, y controles y directrices para la protección a los activos de información.

Seguridad de la documentación producida.

La documentación que se produce en las dependencias puede contener información sensible, por lo que se considerarán almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación al personal estrictamente necesario.

6.8.7. Intercambio de información.

Se establecerán controles de seguridad que ofrezcan seguridad y protección a la información que se está intercambiando, en especial a información sensible. Si esto ocurre, en el acuerdo hecho entre ambas partes deben quedar reflejado responsabilidades y procedimientos para el envío, transmisión, recepción y confirmación.

En este mismo sentido se incluyen controles de autenticación, responsabilidades de propiedad de datos, el establecimiento de registros de auditoría y gestión de incidentes.

Si la información se envía en un soporte mediante correo postal o mensajería, hay que considerar posibles incidentes durante el transporte, tales como accesos indebidos o modificaciones.

6.8.8. Registro de actividad y supervisión

Se realizarán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Las actividades del administrador del sistema y de la red serán registradas. Estos registros serán protegidos y revisados.

Los relojes de todos los sistemas de informáticos relevantes serán sincronizados a una fuente de tiempo de referencia única.

6.8.9. Información públicamente disponible.

Se constituirá una oferta, por medios electrónicos, de información y datos públicos no sensibles y que pueden ser utilizados por terceros según exigencias de Ley

Se habilitará la comunicación de dos vías entre los servidores públicos y la ciudadanía, mediante mecanismos que acercan al ciudadano con la administración y le posibilitan contactarla.

6.8.10. Consideraciones de supervisión y auditoría de sistemas de información

La Secretaria General realizará podrá acceder a la inspección de todos los activos de información para propósitos de auditoría, resolución de problemas o para investigar violaciones a las políticas de seguridad de la información de la Entidad.

Se programarán auditorias operativas de carácter interno a los procesos de gestión tecnológica, gestión documental y seguridad de la información, estas auditorías deberán concluir sobre la eficacia y eficiencia de las plataformas de tecnologías de la información implementados en la Entidad.

6.9. Seguridad de las Telecomunicaciones

Objetivo: Garantizar la protección de la información en las redes y sus instalaciones de apoyo de procesamiento de información.

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red deben ser identificados e incluidos en los acuerdos de servicios de red.

Se definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Entidad, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración de los equipos remoto, incluyendo los equipos en las dependencias de la Entidad.
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
- Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- Garantizar mediante actividades de supervisión, que los controles que aplican uniformemente en toda la infraestructura de procesamiento de información.

6.9.1. Segregación de redes

La plataforma tecnológica de la Entidad que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de datos, de conexiones con redes con terceros y del servicio de acceso a Internet.

6.9.2. Intercambio de información con partes externas

Políticas y procedimientos de intercambio de información

Las políticas formales de transferencia, procedimientos y controles deberán estar en posición de proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

Acuerdos sobre la transferencia de información

La entidad en su intención de proteger la información, indistintamente del lugar o forma en que está se encuentre almacenada, proveerá los recursos necesarios para garantizar la protección de la misma al momento de ser transferida, comunicada a un tercero o al salir de sus instalaciones según necesidad de la actividad o proceso particular.

El intercambio electrónico de información utilizando el canal de internet institucional, se debe realizar con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacional y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad, no repudio y aceptación de la información.

El contenido de los archivos y toda información enviados a través del canal de Internet de la Entidad será directamente responsabilidad del funcionario y/o contratista.

Los responsables del intercambio de información con entidades externas deben definir en compañía de la Secretaria General las estrategias para la correcta gestión e intercambio seguro de la misma.

Mensajería electrónica

La información involucrada en la mensajería electrónica estará debidamente protegida.

Acuerdos de confidencialidad o de no divulgación

Se implementarán los diferentes requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la Entidad para la protección de la información.

Gobierno electrónico.

La entidad implementa acciones dispuestas por el proyecto “GOBIERNO EN LINEA” del Ministerio de tecnologías de la información y las comunicaciones con el objeto de poner a disposición de la ciudadanía información pertinente, veraz, oportuna y accesible en línea, en los procesos de prestación de servicios, toma de decisiones, rendición de cuentas y control social.

6.10. Adquisición, desarrollo y mantenimientos de sistemas de información

Objetivo: Garantizar que la seguridad informática es una parte integral de los sistemas de información a través de todo el ciclo de vida de los sistemas de información.

Se establecerán los procedimientos correspondientes para la adquisición de sistemas de información o aplicación de software, y para el desarrollo o mantenimiento de

software en la Entidad. Para el caso del desarrollo del software subcontratado por la Entidad, se implementarán las supervisiones y metodologías correspondientes.

La Secretaria General como encargada de los sistemas de información brindará la custodia y realizará las copias de los archivos fuente de las aplicaciones de propiedad de la Entidad.

Todos los desarrollos de software y las nuevas aplicaciones que se implementen en la Entidad deben estar autorizados por la Secretaria General.

Los controles y directrices que brinden seguridad y protección al desarrollo y mantenimiento de software harán parte del subsistema de seguridad de la información.

6.10.1. Requisitos de seguridad de los sistemas de información.

Análisis y especificación de los requisitos de seguridad.

En todo desarrollo e implementación, y mantenimiento de los sistemas de información o aplicaciones de software, se identificarán, especificarán y analizarán los requerimientos de seguridad.

Con base en el análisis y clasificación del riesgo del sistema y durante la fase de diseño del proyecto, los requerimientos de seguridad deberán ser definidos formalmente por parte del "usuario" del sistema o un representante del mismo. Las medidas de seguridad deben ser definidas a partir de los requerimientos de seguridad establecidos.

6.10.2. Tratamiento correcto de las aplicaciones

Validación de los datos de entrada.

Se identificará cada uno de los flujos de entrada de datos y se verificará que el tipo de datos sea el esperado. Los controles y su tratamiento serán documentados.

Control del procesamiento interno.

En el diseño de los sistemas de información y aplicaciones contemplará la implementación de controles para la verificación de requisitos previos al procesamiento de información, adicionales a los controles manuales que se dispongan.

Todo procesamiento contará con mecanismos de recuperación ante fallas para garantizar la integridad de la información en los sistemas y aplicaciones afectadas. Se considerarán mecanismos de reprocesamiento de información con su respectivo registro de trazabilidad de las operaciones realizadas.

Integridad de los mensajes.

Se identificarán los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, los cuales hacen referencia al estado y finalización de transacciones, petición de datos, solicitud de acciones al usuario, petición de claves, confirmaciones, errores, resultados de validaciones, entre otros; se identificarán e implantarán los controles apropiados

Validación de los datos de salida.

Se establecen mecanismos como casos de prueba para verificar la salida esperada de datos en informes, reportes o consultas, por el proceso o los usuarios.

6.10.3. Controles criptográficos.

Política de uso de los controles criptográficos.

Se utilizarán controles criptográficos en los siguientes casos:

- Para los sitios web de uso externo, como por ejemplo página web institucional.
- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada como crítica o sensible, fuera del ámbito de la Entidad
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

6.10.4. Seguridad de los archivos de sistema.

Control del software en explotación.

Los sistemas de información y aplicaciones implementadas en la Entidad tendrán un líder técnico responsable designado formalmente por la Secretaria General.

Los desarrolladores software encargados del desarrollo y mantenimiento de aplicaciones no podrán acceder a los ambientes de producción.

La entidad contará con un administrador de despliegues de aplicaciones, quién coordinará la implementación de ajustes y nuevas funcionalidades, para asegurar que los sistemas en producción sean los probados y autorizados por los responsables de las áreas funcionales. El administrador no podrá ser un desarrollador, ni tendrá acceso al código fuente de las aplicaciones, en cumplimiento de la política de segregación de tareas y funciones.

Se contará con la documentación de seguridad que contemple registro de auditoría de las actualizaciones realizadas, retención de las versiones previas del sistema como medida de contingencia y pruebas a realizarse, entre otros.

Protección de los datos de prueba del sistema.

Las pruebas de los sistemas se podrán efectuar sobre datos extraídos del ambiente de producción. En el ambiente de pruebas se aplicarán idénticos procedimientos de control de acceso a los realizados en el ambiente de producción.

Toda copia de información o bases de datos de producción para la realización de pruebas, contará con la autorización de su propietario donde se especifique la fecha de vencimiento de uso. Una vez finaliza esa fecha, la información será eliminada inmediatamente.

Control de acceso al código fuente de las aplicaciones de software.

La Secretaria General definirá e implementará la herramienta para control del código fuente de las aplicaciones de software.

Se designará un responsable para la administración del código fuente de los programas, quién no debe cumplir con funciones de desarrollo mantenimiento o implementación de aplicaciones.

El administrador del código fuente de los programas no deberá realizar modificaciones sobre los programas fuentes bajo su custodia.

Se definirá o actualizará el procedimiento de gestión del código fuente hasta su despliegue en producción, para evitar su alteración y modificación sin los accesos permitidos.

Se establecerá que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

Se prohíbe el acceso a todo operador y/o usuario de aplicaciones a las herramientas que permitan la generación o gestión de los programas fuentes.

Los programas fuentes contarán con copias de respaldo periódicas, cumpliendo los requisitos de seguridad establecidos por la Entidad.

6.10.5. Seguridad en los procesos de desarrollo y soporte.

Procedimientos de control de cambios.

Todo cambio deberá ejecutarse conforme al procedimiento de control de cambios que establezca la Entidad, con el fin de minimizar los riesgos de alteración de los sistemas de información.

Se actualizará la documentación de usuario final o técnica para cada cambio implementado que implique modificaciones en la estructura de la base de datos, cambio de modelo operativo, adición de nueva funcionalidad, entre otros.

Cuando se cambien las plataformas de operación o sistemas operativos, las aplicaciones y sistemas de información deberán ser revisadas y probadas para asegurar que no hay impacto negativo en las operaciones de la Entidad o de la seguridad.

Desarrollo tercerizado

La Secretaria General debe contar con un responsable de autorizar la creación, adaptación o adquisición de software.

Los contratos de consultoría, y en general todo tipo de contratos de servicios deben contener provisiones a este respecto. De igual manera, dada la proliferación del "outsourcing", es especialmente importante clarificar los derechos generados por proveedores en desarrollo de este tipo de contratos.

Pruebas de funcionalidad durante el desarrollo de los Sistemas

Las pruebas de la funcionalidad se deben llevar a cabo durante el desarrollo del sistema.

Pruebas de aceptación del sistema

Se debe cumplir con los formatos y el procedimiento del sistema de calidad para la realización y documentación de las pruebas.

Protección de los datos de prueba

Los datos de prueba deben seleccionarse cuidadosamente, en caso de seleccionar datos reales estos deben ser protegidos y controlados.

6.11. Relación con los proveedores

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores:

6.11.1. Seguridad de la información en relación con los proveedores

Política de seguridad de la información para las relaciones con proveedores

Se acordará con el proveedor y se documentaran los requerimientos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de información de la Entidad.

De igual forma se debe incluir un acuerdo formal de Niveles de Servicios en Seguridad de la Información, en el que se detallen los compromisos en el cuidado de los Activos de Información de la Entidad y las sanciones en caso de incumplimiento. Cuando la supervisión sea contratada, se debe incluir esta obligación dentro de los Contratos.

Tratamiento del riesgo dentro de acuerdos con proveedores

Todos los requerimientos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información de la Entidad.

Cadena de suministro en tecnologías de la información y comunicaciones

Incluir los requerimientos para los acuerdos con proveedores para abordar los riesgos de la seguridad de la información asociada con los servicios de las tecnologías de información y comunicación y de la cadena de suministro de productos.

6.11.2. Gestión de la prestación de servicios por proveedores

Seguimiento y revisión de los servicios de proveedores

Cada servicio con proveedor deberá tener con un supervisor encargado de revisar y auditar la prestación de servicios de proveedores.

Gestión de cambios en los servicios prestados por proveedores

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y re-evaluación de los riesgos.

6.12. Gestión de incidentes de seguridad

Objetivo: Garantizar un enfoque coherente y eficaz para la gestión de incidentes en la seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la Información.

Todo funcionario y contratista de la Entidad es responsable del reporte oportuno de debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su

comunicación al Comité de Seguridad de la Información y a los propietarios de la información.

El Comité de Seguridad efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable de Seguridad de la Información junto con la Secretaria General son los responsables de establecer el proceso, procedimientos e instructivos para la Gestión de Incidentes de Seguridad de la Información

6.12.1. Gestión de incidentes y mejoras de seguridad de la información

Notificación de eventos y puntos débiles de seguridad de la información.

Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, soporte técnico, entre otros. Toda persona de la Entidad deberá reportar de manera oportuna las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.

Responsabilidades y procedimientos.

La responsabilidad y el procedimiento de manejo para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información está en cabeza de la Secretaria General. El procedimiento debe contemplar el reporte, registro, clasificación, diagnóstico, resolución y cierre del incidente, así como el monitoreo y seguimiento del incidente.

Aprendizaje de los incidentes de seguridad de la información.

La solución de un incidente se registrará en una base de conocimientos de errores conocidos, con el fin de que pueda ser consultada y sirva de apoyo oportuno cuando un incidente se presente de manera recurrente o de pistas de solución en incidentes similares. La recurrencia de un incidente deberá ser tratada como un problema. Asi como para reducir la probabilidad o el impacto de los incidentes en el futuro.

Recopilación de evidencia

Se deberá registrar las pistas de auditoría y evidencias para análisis de problemas internos, uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial y negociación de compensaciones por parte de los proveedores de software y de servicios.

Respuesta a vulnerabilidades e Incidentes Relativos a la Seguridad

La Entidad desarrollará un procedimiento formal de comunicaciones, que incluya el reporte, verificación, escalamiento, seguimiento, acciones de mejoras y cierre de vulnerabilidades, riesgos o incidente de seguridad que se detecten o sucedan.

Todos funcionarios y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

Documentación de los Incidentes

La Entidad deberá documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Identificará aquellos que sean recurrentes, con su respectivo de nivel de impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

6.13. Gestión de la Continuidad del negocio

Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.

Los directores, Jefes de área y el responsable de Seguridad de la Información identificaran las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la Entidad, evaluaran los riesgos para determinar el impacto de dichas interrupciones, Identificar los controles preventivos, elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades.

Para los procesos críticos de la entidad, se debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de operación.

El plan de continuidad debe considerar los siguientes aspectos:

- Plan de contingencia. Los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.
- Plan de recuperación. Los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.
- Plan de retorno. Los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.
- Programación de pruebas. Las cuales describen la periodicidad en que el plan de continuidad debe ser probado.
- Actualización periódica. El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad.
- Consideraciones de seguridad. Es importante que el plan sea diseñado para mantener los controles de seguridad establecidos por la Organización, aun cuando

se opere en modalidad de contingencia. Es responsabilidad del responsable de la seguridad de la información asegurar que estas consideraciones sean efectivamente contempladas en el plan.

6.13.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

La Entidad debe contar con un procedimiento de gestión de la continuidad del negocio, que contemple la implementación y actualización de planes de contingencia para garantizar que las operaciones de la Entidad puedan restablecerse dentro de plazos aceptables, ante la eventual ocurrencia de interrupciones de actividades

La Secretaria General desarrollará un plan de contingencias informáticas y de comunicaciones, el cual estará ajustado a los estándares nacionales e internacionales.

Planificación de la continuidad de la seguridad de la información y Análisis de riesgos

Se realizará análisis de riesgos enfocado específicamente a valorar el impacto de incidentes que comprometen la continuidad del negocio teniendo en cuenta que este impacto será mayor cuanto más dure el incidente. Se definirán los pasos a seguir para realizar el análisis de riesgos.

Implantación de la continuidad de la seguridad de la información

Establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información

El Comité de Seguridad de Información establecerá y hará seguimiento al cronograma de pruebas periódicas de cada plan de contingencia, para minimizar el riesgo de fallas por cambios en la infraestructura, por errores o malas apreciaciones y definiciones

Redundancias

Las instalaciones para el procesamiento de información deben contar con la suficiente redundancia para satisfacer los requisitos de disponibilidad.

6.14. Cumplimiento

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.

El Comité de Seguridad de la Información debe garantizar el cumplimiento de las directrices definidas en la presente Política de Seguridad de la Información.

Los directores y Jefes de área velarán por la correcta implementación y cumplimiento de la Política de Seguridad de la Información, y los controles y directrices de seguridad que harán parte del Subsistema de Seguridad de la Información, dentro de la dependencia de su responsabilidad.

Las situaciones o acciones que violen la presente Política, controles y directrices deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

6.14.1. Cumplimiento de los requisitos legales.

Identificación de la legislación aplicable

En el numeral 4. Marco legal de la presente política, se encuentra relacionada la legislación aplicable a la seguridad de la información.

Derechos de propiedad intelectual

La Entidad solo podrá autorizar para la realización de sus actividades el uso software licenciado, software desarrollado en la Entidad o software declarado como de libre uso, asi mismo, uso de material documental, el producido por la Entidad misma o el producido por el titular cuando medie autorización de este, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente. Los funcionarios únicamente podrán utilizar material o software autorizado por la Entidad.

Se debe establecer en los contratos de trabajo de empleados y en los contratos de realizados con proveedores y contratistas, cláusulas respecto a la propiedad intelectual respecto, al material y productos generados en el desarrollo del negocio.

Protección de los documentos de la organización.

Los documentos críticos de la Entidad se protegerán contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales. Para cada uno de ellos se debe detallar los períodos de retención y el tipo de medios de almacenamiento, por ejemplo, papel, microfichas, medios magnéticos u ópticos. Para esto se debe cumplir con los lineamientos y directrices fijadas por la Entidad y por el Archivo General de la Nación.

Protección de datos y privacidad de la información de carácter personal

Los funcionarios y contratistas de la Entidad deberán conocer las restricciones al tratamiento de los datos y de la información personal registrada en la Entidad, conforme

a lo estipulado en la normatividad interna y en la Ley Estatutaria 1581 de 17 de octubre 2012, por la cual se dictan disposiciones para la protección de datos personales: "T*odas las personas tiene el derecho constitucional a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".*

Prevención del uso indebido de recursos de tratamiento de la información

Los funcionarios y contratistas de la Entidad deben conocer y respetar el alcance preciso del uso adecuado de los recursos informáticos.

Regulación de los controles criptográficos

Los controles criptográficos serán utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.

6.14.2. Revisiones de la seguridad de la información

Revisión independiente de la seguridad de la información

El enfoque de la Entidad para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisará de forma independiente a los de demás procesos de la Entidad a intervalos planificados o cuando se produzcan cambios significativos.

Cumplimiento de las políticas y normas de seguridad

La Secretaria General deberá comprobar periódicamente el cumplimiento de los procesos y procedimientos de la información relacionados con la seguridad de la información e informar el cumplimiento al Comité de Seguridad de la Información, quien tomará las medidas según sea el caso para la mejora continua.

Comprobación del cumplimiento

Los Activos de información deben ser revisados regularmente para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

Las situaciones o acciones que quebranten la presente Política deben ser detectadas, registradas, analizadas, resueltas e informadas al comité de Seguridad de la Información y a las áreas responsables por su tratamiento de manera inmediata.