MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad y Privacidad de la Información

Fase Planificación

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL MINISTERIO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
POLÍTICA DE GOBIERNO DIGITAL.

ABRIL DE 2018

FORMATO PRELIMINAR AL DOCUMENTO

Título:	**MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**				
Fecha de elaboración	18 - 04 - 2018				
Sumario	Este documento contiene las Políticas de Seguridad y Privacidad de la Información adoptadas por LA EMPRESA DE ASEO DE PEREIRA S.A. ESP, a través de la "Política General de Seguridad y Privacidad de la Información" para la implementación del "Sistema de Gestión de Seguridad y Privacidad de la Información".				
Palabras Claves	Sistema de Gestión Seguridad de la Información Privacidad de la Información Norma ISO 27001:2013				
Formato:	PDF y DOC		Lenguaje:	Español	
Dependencia:	Comité Directivo				
Código:	N/A	Versión	1.0	Estado	En Aprobación
Categoría	Documento Técnico, Implementación de la Política de Gobierno Digital en LA EMPRESA DE ASEO DE PEREIRA S.A. ESP: Habilitante: Seguridad y Privacidad de la Información Logro: Definición del Marco de Seguridad y Privacidad de la Información Criterio: Plan de Seguridad y Privacidad de la Información Subcriterio: La entidad define las acciones a implementar a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo. Herramientas: NTC-ISO-IEC 27001:2013, M.SPI Modelo de Seguridad y Privacidad de la Información para GEL – Guía 2 Elaboración de la política general de seguridad y privacidad de la información. – Guía 4 Roles y Responsabilidades.				
Autor (es):	Magister CARLOS MARIO ARTEAGA PACHECO, Contratista Ingeniero ORLANDO ZAPATA ALVAREZ Contratista				
Revisó:	Comité Institucional de Gestión y Desempeño				
Aprobó:	Comité Institucional de Gestión y Desempeño				

CONTENIDO

Pag

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Política de Gobierno Digital incluye en los habilitantes Transversales la Seguridad de la Información, razón por la cual, la EMPRESA DE ASEO DE PEREIRA S.A. ESP inició la implementación de un Modelo de Seguridad y Privacidad de la Información, a través del cual la información sea protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este manual compila y detalla las Políticas de Seguridad de la Información adoptadas por la EMPRESA DE ASEO DE PEREIRA S.A. ESP a través de la Política General de Seguridad y Privacidad de la Información. Para la elaboración del mismo, se tomaron como base las normas aplicables en Colombia sobre Seguridad y Privacidad de la Información, el Modelo de Privacidad y Seguridad de la Información del Ministerio de las Tecnologías de Información y Comunicaciones, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las Políticas incluidas en este manual se constituyen como parte fundamental del Sistema de Gestión de Seguridad y Privacidad de la información de la EMPRESA DE ASEO DE PEREIRA S.A. ESP y se convierten en la base para la implantación de los controles, procedimientos y estándares requeridos.

1 OBJETIVO

Este MANUAL establece los lineamientos de implementación de las Políticas en Seguridad de la Información de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, con el fin de gestionar la seguridad de la información al interior de la entidad.

2 ALCANCE

Las Políticas de Seguridad de la Información cubren todos los lineamientos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la EMPRESA DE ASEO DE PEREIRA S.A. ESP, para el logro de un adecuado nivel de protección de las características de seguridad y privacidad de la información relacionada.

3 DEFINICIONES

Activo de información: Cualquier componente de información preservado a través de un medio humano, tecnológico, software, documental o de infraestructura y al cual se le asigna valor económico, legal o estratégico para los procesos de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, y en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en el que las personas vinculadas a la EMPRESA DE ASEO DE PEREIRA S.A. ESP o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un activo de información protegido.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: Es la unidad organizacional o proceso, designado por la EMPRESA DE ASEO DE PEREIRA S.A. ESP, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes a la EMPRESA DE ASEO DE PEREIRA S.A. ESP

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: Es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo en la EMPRESA DE ASEO DE PEREIRA S.A. ESP

Registros de Auditoría: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la EMPRESA DE ASEO DE PEREIRA S.A. ESP Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por la EMPRESA DE ASEO DE PEREIRA S.A. ESP, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la EMPRESA DE ASEO DE PEREIRA S.A. ESP.

Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la EMPRESA DE ASEO DE PEREIRA S.A. ESP (amenazas), las cuales se constituyen en fuentes de riesgo.

4 POLÍTICA: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene como finalidad establecer el Comité Directivo de la Seguridad de la Información.

Es necesario que las responsabilidades asignadas en el desarrollo del proyecto del SGSPI para cada perfil, sean incorporadas a los manuales de funciones de acuerdo al cargo que desempeñan.

4.1 CONFORMACIÓN DEL COMITÉ DIRECTIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4.1.1 Objetivos del Comité:

El Comité Directivo de Seguridad y Privacidad de la Información se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades que tengan lugar para adoptar el Modelo de Seguridad y Privacidad de la Información al interior de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, así como planear las actividades proyectadas para una adecuada administración y sostenibilidad del mismo.

4.1.2 Miembros del Comité

El Comité Institucional de Gestión y Desempeño de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, realizará las funciones de Comité de Seguridad y Privacidad de la Información, acorde con lo establecido en la función número 6, asignada en el Artículo 2.2.22.3.8 de la Ley 1499 de 2017 (6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información), y el numeral 5.1 LIDERAZGO Y COMPROMISO; de la norma NTC-ISO-IEC 27001:2013.

El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

4.1.3 Funciones del Comité

a) Discutir y Coordinar todas las actividades tendientes a la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información.

b) Revisar los diagnósticos del estado de la seguridad de la información.

c) Aprobar e implementar la Política General de Seguridad y Privacidad de la Información.

d) Revisar periódicamente el documento de la Política de Seguridad y Privacidad de la Información.

e) Procurar por el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

f) Establecer los roles y responsabilidades de las personas que se van a encargar de la ejecución de cada una de las actividades asociadas a la implementación del SGSPI.

g) Acompañar e impulsar el desarrollo de proyectos de seguridad.

h) Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.

i) Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

j) Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

k) Verificación el avance de las diferentes etapas del Sistema de Gestión de Seguridad y Privacidad de la Información.

l) Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

m) Comunicar y socializar al interior de la organización EMPRESA DE ASEO S.A. ESP, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

n) Verificar el cumplimiento de las Políticas de Seguridad y Privacidad de la Información.

o) Las demás funciones inherentes a la naturaleza del Comité.

4.1.4 Secretaria Técnica

La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada doce (12) meses.

4.1.5 Funciones de la Secretaría Técnica.

Las funciones de la Secretaría Técnica serán las siguientes:

1) Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2) Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3) Remitir oportunamente a los miembros la agenda de cada comité.
4) Llevar la custodia y archivo de las actas y demás documentos soportes.
5) Servir de interlocutor entre terceros y el Comité.

6) Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7) Presentar los informes que requiera el Comité.
8) Las demás que le sean asignadas por el Comité.

4.1.6 Reuniones del Comité de Seguridad y Privacidad de la Información.

El Comité de Seguridad y Privacidad de la Información deberá reunirse (según periodicidad definida por el Comité Institucional de Gestión y Desempeño), previa convocatoria del Secretario Técnico del Comité.

4.1.7 Sesiones Extraordinarias

Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo a temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

4.2 ROL: Responsable de Seguridad de la información

Se desempeñará como líder del proyecto de Seguridad y Privacidad de la Información en la EMPRESA DE ASEO DE PEREIRA S.A. ESP.

Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de Arquitectura Empresarial (IT4+), está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo al Dominio:

Tabla No. 1 Responsabilidades – Marco de Arquitectura Empresarial[1]

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. - Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. - Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. - Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. - Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para

[1] Guia No 4 ROLES Y RESPONSABILIDADES, Modelo de Seguridad y Privacidad de la Información. Ministerio de las Tecnologías de Información y Comunicaciones

DOMINIO	RESPONSABILIDADES
	detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	- Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. - Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	- Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. - Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. - Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. - Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. - Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
INFORMACIÓN	- Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. - Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
USO Y APROPIACIÓN	- Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. - Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. - Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

El Responsable de Seguridad de la Información es responsable de entregar y dar a conocer los perfiles y responsabilidades de cada rol al Grupo Operativo de Seguridad de la Información, según los roles asignados.

4.3 Grupo Operativo de Seguridad de la información

El modelo establece la conformación de un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la EMPRESA DE ASEO S.A. ESP esté disponible oportunamente.

De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la EMPRESA DE ASEO S.A. ESP, y que no dependa exclusivamente de la oficina o área de TI

Estará conformado por:

1) Un representante del área Administrativa.
2) Un representante del área de Tecnología.
3) Un representante del área de Control Interno.
4) Un representante de Sistemas de Gestión de Calidad.
5) Un representante del Área Jurídica.

Será Liderado por el Responsable de Seguridad de la Información.

Responsabilidades del Grupo Operativo de seguridad de la Información:

1) Apoyar al Responsable de Seguridad de la Información al interior de la entidad.
2) Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
3) Ayudar al Responsable de Seguridad de la Información designado, en la gestión de proveedores de tecnología e infraestructura.
4) Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el Responsable de Seguridad de la Información.
5) Las que considere el Responsable de Seguridad de la Información del proyecto o el Comité de Seguridad y Privacidad de la Información de la EMPRESA DE ASEO DE PEREIRA S.A. ESP.

4.3.1.1 Responsables de Tratamiento de Datos Personales

La Ley 1581 de 2012 sobre Protección de Datos Personales los define cómo: 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.

De acuerdo a la Ley 1581 de 2012 los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

1) Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
2) Tramitar las consultas, solicitudes y reclamos.
3) Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
4) Respetar las condiciones de seguridad y privacidad de información del titular.
5) Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

5 POLÍTICA: POLÍTICAS DE SEGURIDAD DEL PERSONAL

5.1 POLÍTICA RELACIONADA CON LA VINCULACIÓN DE PERSONAL

El Proceso Administrativo debe garantizar que las personas que se vinculan a la nómina de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad y Privacidad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

En el caso de contratistas o personal provistos por terceras partes:

Los contratistas de prestación de servicios, así como el personal provisto por terceras partes que realicen labores en o para la EMPRESA DE ASEO DE PEREIRA S.A. ESP, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad y Privacidad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

Cada Supervisor de Contrato, debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de Aceptación de Políticas de Seguridad y Privacidad de la Información antes de otorgar acceso a la información de la EMPRESA DE ASEO DE PEREIRA S.A. ESP.

5.2 POLÍTICA DE DESVINCULACIÓN DE PERSONAL

La EMPRESA DE ASEO DE PEREIRA S.A. ESP asegurará que sus funcionarios, empleados, contratistas de prestación de servicios y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

En el caso de desvinculación de personal de planta, licencias, vacaciones o cambio de labores de los funcionarios o empleados de planta, el Proceso Administrativo verificará el cumplimiento del proceso de devolución de activos de información asignados, ejecutando los controles establecidos para tal fin.

En el caso de contratistas de prestación de servicios y el personal provisto por terceros, el o los Supervisores o interventores de Contrato, debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los contratistas de prestación de servicios o personal provistos por terceras partes al Proceso Administrativo, adjuntando los correspondientes formatos de certificación de devolución de activos de información.

Cada Supervisor o interventor de Contrato, de debe verificar la entrega por parte del contratista de las cuentas institucionales de acceso a los sistemas de información, a través del formato definido para tal fin.

6 POLÍTICA: GESTIÓN DE ACTIVOS DE INFORMACIÓN

6.1 IDENTIFICACIÓN DE ACTIVOS

La EMPRESA DE ASEO DE PEREIRA S.A. ESP mantendrá el inventario de activos de información mediante el formato normalizado "Inventario De Activos De Información" en medio digital. Este inventario se actualizará cada vez que se presenten modificaciones a la plataforma tecnológica de sistemas de información, el archivo físico, o se implementen procesos o procedimientos nuevos en la EMPRESA DE ASEO DE PEREIRA S.A. ESP.

El formato normalizado contendrá:

Datos de identificación del activo, descripción del activo, localización física del activo, propietario del activo, responsable de la seguridad del activo, estado del activo, clasificación del activo de acuerdo a la criticidad, sensibilidad y reserva.

La actualización y conservación del Inventario de Activos de Información estará a cargo del Proceso de Gestión Administrativa, acorde con el procedimiento, los protocolos y registros que para tal efecto se registren y normalicen en el Sistema de Gestión de la Calidad.

6.2 ETIQUETADO DE LA INFORMACIÓN

El etiquetado o rotulación de Activos de Información se desarrollará bajo los lineamientos del Proceso de Gestión Administrativa y el Proceso registrado para tal efecto en el Sistema de Gestión de la Calidad.

6.3 DEVOLUCIÓN DE LOS ACTIVOS

Para los funcionarios o empleados de Planta o con contrato a término indefinido, los activos de información harán parte del inventario a su cargo y serán entregados mediante el proceso o protocolo de entrega de inventario al momento de tomar posesión del puesto o cargo.

La devolución o entrega de activos de información por estos funcionarios o empleados de planta, se realizará siguiendo los procedimientos para devolución o descarga de activos establecidos en el Proceso de Gestión Administrativa.

Para los contratistas de prestación de servicios, la entrega de activos de información requeridos para el desarrollo del contrato, se hará a través del formato "Entrega de Activos de Información a Contratistas", previa verificación de la suscripción del formato "Acuerdo de confidencialidad y protección de activos de información".

Los Activos de Información suministrados a Contratistas serán devueltos al finalizar el contrato en el acto de Liquidación del Contrato, mediante el formato "Devolución de Activos de Información por parte de Contratistas".

6.4 GESTIÓN DE MEDIOS REMOVIBLES

Sólo le está permitido el uso de dispositivos removibles cómo memorias USB, discos duros externos, memorias SD entre otros, al personal de planta o contratista que en desarrollo de su función o actividad así lo requiere y no sea posible recurrir a medios como el correo electrónico para la entrega o desplazamiento de la información.

En todos los casos, el dispositivo será sometido a revisión de antivirus, se verificará además el cumplimiento del Protocolo de entrega de información en medios removibles a funcionarios, contratistas o terceros.

En caso de que medien datos personales, se debe verificar las autorizaciones del **titular de la información** y del **responsable del tratamiento** en los términos de la Ley 1581 de 2012.

6.5 DISPOSICIÓN DE LOS ACTIVOS

La EMPRESA DE ASEO DE PEREIRA S.A. ESP a través del Proceso de Gestión Administrativa construirá y dará cumplimiento a un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o reuso cuando ya no se requieran los activos. El procedimiento determinará la toma de copia de seguridad (*backup*) de los activos evitando así el acceso o borrado no autorizado de la información. De igual forma, el procedimiento indicará quién es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

6.6 DISPOSITIVOS MÓVILES

La EMPRESA DE ASEO DE PEREIRA S.A. ESP Dispondrá de servicios de Redes inalámbricas para conexión de dispositivos móviles, separando los flujos del servicio público de los servicios de intranet, manteniendo separados los flujos de terceros y visitantes de los flujos de funcionarios y contratistas de la entidad.

Los funcionarios y contratistas de la entidad tendrán acceso móvil a la intranet para el desarrollo de sus funciones o actividades contratadas, en este caso, los dispositivos serán registrados en la red a través de su identificación MAC y en lo posible se asignará una dirección IP fija para su identificación.

Todos los dispositivos que se conecten de forma móvil deberán contar con la autorización del superior inmediato o el interventor o supervisor según proceda, siguiendo el Protocolo para uso de servicios móviles en la Intranet, a través del formato "Registro e ingreso de dispositivos móviles a la intranet"

Los funcionarios o contratistas que utilizan la intranet a través de los servicios móviles asumen la responsabilidad descrita en el compromiso de confidencialidad y privacidad de la información suscrito con la EMPRESA DE ASEO DE PEREIRA S.A. ESP frente al uso de la información almacenada en los dispositivos móviles así como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

7 POLÍTICA: CONTROL DE ACCESO DIGITAL

7.1 CONTROL DE ACCESO CON USUARIO Y CONTRASEÑA

La EMPRESA DE ASEO DE PEREIRA S.A. ESP aplicará el control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad, a través de los procedimientos y protocolos de control de acceso que se determinen en los respectivos Procesos responsables de la seguridad de los activos de información. Estos procedimientos definen el mecanismo formal de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas.

Los funcionarios, contratistas o terceros, al contar con un usuario o contraseña de la entidad, asumen la responsabilidad por cualquier uso debido o indebido que se haga de la misma. Los usuarios (ID) y contraseñas son personales e intransferibles y no se pueden prestar, ni compartir. Por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso, las cuales deberán ser entregadas al final de la vinculación acorde al protocolo establecido en la política de desvinculación de personal.

7.2 SUMINISTRO DE USUARIO (ID) PARA ACCESO DIGITAL

El Proceso de Gestión Administrativa de la EMPRESA DE ASEO DE PEREIRA S.A. ESP determinará los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados.

Los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad, deberán consignarse en sobres sellados y depositarse en caja fuerte de la entidad cómo medida de contingencia ante ausencia forzosa del titular del usuario y la necesidad de acceso para la continuidad de las operaciones de la EMPRESA DE ASEO DE PEREIRA S.A. ESP.

7.3 GESTIÓN DE CONTRASEÑAS PARA USUARIO (ID) DIGITAL

Las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.

En todos los casos, las contraseñas deben seguir las siguientes reglas mínimas de seguridad:

a) Longitud igual o superior a 8 caracteres.
b) Se debe combinar letras y números.
c) En el cambio periódico de contraseña deben cambiar por lo menos 4 de los caracteres.

En la creación de un usuario nuevo, se le dará una contraseña genérica y el sistema identificará que es su primer ingreso y obligará el cambio de contraseña antes de ingresar.

Las contraseñas de acceso a servicios básicos de red e intranet deben ser renovadas con una periodicidad semestral. El cambio debe ser forzado por la plataforma en el primer ingreso del usuario después de vencido el plazo.

Las contraseñas de acceso a los sistemas de información deben ser renovadas con una periodicidad semestral. El cambio debe ser forzado por la plataforma en el primer ingreso del usuario después de vencido el plazo.

Los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad, deben ser cambiadas y el sobre renovado con una periodicidad máxima semestral.

7.4 PERÍMETROS DE SEGURIDAD

Se establece cómo perímetros físicos con acceso restringido a **funcionarios, contratistas y terceros** los siguientes:

a) Data Center Principal ubicado en el sexto (6) piso de la Unidad Administrativa el Lago.
b) Área de Archivo Físico Central ubicada en la Unidad Administrativa el Lago.

El acceso a estas áreas está sujeto a la autorización del Líder de Proceso, según los protocolos adoptados.

Se establece cómo perímetro físico con acceso restringido a **terceros y visitantes**:

a) Las áreas de puestos de trabajo de funcionarios.

El acceso a esta área lo autoriza el funcionario responsable del puesto de trabajo, según el protocolo adoptado.

Se establece cómo perímetros con acceso libre a **visitantes y terceros**:

a) Áreas de espera.
b) Instalaciones sanitarias.

El acceso a esta área lo autoriza el funcionario responsable del puesto de trabajo de recepción o Secretaria de Gerencia, según el protocolo adoptado.

8 POLÍTICA: NO REPUDIO

8.1 TRAZABILIDAD

A través de los registros del Sistema de Gestión de la Calidad, el MECI y el Sistema de Gestión de Seguridad y Privacidad de la Información, se hará la trazabilidad de las acciones de creación, origen, recepción, entrega de información y otros.

8.2 RETENCIÓN

El periodo de retención o almacenamiento de las acciones realizadas por los usuarios, estará definido a través de las tablas de retención documental del Sistema de Gestión Documental (Archivo) de la EMPRESA DE ASEO DE PEREIRA S.A. ESP y será informado a los funcionarios, contratistas y/o terceros de la Entidad.

8.3 AUDITORÍA

La plataforma tecnológica de los sistemas de información mantendrá activas las acciones de registro y trazas de auditoría, para la realización de auditorías continuas, en concordancia con las auditorías del sistema de calidad y del MECI, como procedimiento para asegurar la trazabilidad en caso de que las partes implicadas nieguen haber realizado una acción.

8.4 INTERCAMBIO ELECTRÓNICO DE INFORMACIÓN

El Proceso de Gestión Administrativa de la EMPRESA DE ASEO DE PEREIRA S.A. ESP desarrollará los procedimientos y protocolos en los casos que aplique, para los servicios de intercambio electrónico de información con garantía de no repudio.

9 POLÍTICA: PRIVACIDAD Y CONFIDENCIALIDAD

Esta política contiene una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente.

9.1 ÁMBITO DE APLICACIÓN

Todos los datos que por su característica se encuentren clasificados como datos personales o datos sensibles, en los términos de la Ley 1581 de 2012 y sus Decretos reglamentarios.

9.2 PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

- **Principio de la Legalidad**: El tratamiento de datos personales se hace bajo los parámetros de la Ley 1581 de 2012 y sus Decretos reglamentarios.

- **Principio de finalidad**: en el caso de los usuarios la información recopilada será utilizada para cálculos estadísticos relacionados con la prestación del servicio de transporte masivo. En el caso de funcionarios y contratistas la información se utilizará para los trámites propios de la relación laboral cómo el pago de nóminas, honorarios, reportes a entes de control y fiscalización. La finalidad será informada al titular en el momento mismo de la recolección consentida de la información.

- **Principio de libertad**: El tratamiento sólo se realizará con el consentimiento previo, expreso e informado del titular de los datos.

- **Principio de veracidad o calidad**: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

- **Principio de transparencia**: La EMPRESA DE ASEO DE PEREIRA S.A. ESP garantizará al titular de los datos el derecho a obtener la información registrada que le concierna.

- **Principio de acceso y circulación restringida**: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.

- **Principio de seguridad**: La EMPRESA DE ASEO DE PEREIRA S.A. ESP manejará la información sujeta a tratamiento con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

- **Principio de confidencialidad**: Todas las personas que participen en el Tratamiento de Datos Personales garantizarán la reserva de dicha información

9.3 DERECHOS DE LOS TITULARES

Acorde con la Ley 1581 de 2012, la EMPRESA DE ASEO DE PEREIRA S.A. ESP reconoce los derechos de los titulares de los datos, así:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- Ser informado respecto del uso que se les da a sus datos personales.
- Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes los servicios o productos que dieron origen a dicha autorización.
- Presentar quejas ante la entidad administrativa (Superintendencia de Industria y Comercio) encargada de la protección de los datos personales.

9.4 AUTORIZACIÓN DEL TITULAR

La autorización del titular se obtendrá de forma informada, para ello la EMPRESA DE ASEO DE PEREIRA S.A. ESP dejará en todos los formatos donde se recoja o recopile datos personales, el párrafo informativo que mencionará la Ley de protección de Datos Personales e indicará el tratamiento del cual serán objeto, la autorización del tratamiento quedará refrendada con la firma del titular en el formato físico, o con el diligenciamiento por medios electrónicos por parte del titular, según corresponda.

9.5 DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO (Ley 1581 de 2012)

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

m) Informar a solicitud del Titular sobre el uso dado a sus datos.

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

9.6 DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO (Ley 1581 de 2012)

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración. pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley 1581 de 2012.

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la Ley 1581 de 2012.

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley 1581 de 2012 y, en especial, para la atención de consultas y reclamos por parte de los Titulares.

g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley 1581 de 2012.

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

9.7 COMPROMISO O ACUERDO DE CONFIDENCIALIDAD

El Proceso de Gestión Administrativa desarrollará el protocolo y formato de Compromiso de Confidencialidad por medio del cual todo funcionario, contratista y/o tercero vinculado a la EMPRESA DE ASEO DE PEREIRA S.A. ESP, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

El formato de acuerdo indicará desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

10 POLÍTICA: INTEGRIDAD

Los funcionarios, contratistas y/o terceros que hacen parte de la EMPRESA DE ASEO DE PEREIRA S.A. ESP deberán conocer y aceptar el manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos, mediante la aplicación de los lineamientos del Sistema de Gestión de la Calidad y el MECI.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de “Cláusula de integridad de la información”.

El compromiso de integridad, deberá establecer asimismo la vigencia del mismo acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

11 POLÍTICA: DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La EMPRESA DE ASEO DE PEREIRA S.A. ESP contará con un Plan de Continuidad del Servicio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La EMPRESA DE ASEO DE PEREIRA S.A. ESP trabajará en procura de garantizar los siguientes parámetros:

11.1 NIVELES DE DISPONIBILIDAD

La EMPRESA DE ASEO DE PEREIRA S.A. ESP velará por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con usuarios, proveedores y/o terceros en función de las necesidades de la Entidad, los niveles de servicios en ningún caso serán inferiores al 90%.

11.2 PLANES DE RECUPERACIÓN

Los Procesos de la EMPRESA DE ASEO DE PEREIRA S.A. ESP elaborarán sus planes de recuperación de Desastres para hacer frente a:

- **Interrupciones:** Los Procesos deben velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad del mismo.

- **Acuerdos de Nivel de servicio:** Los Procesos deben tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.

- **Segregación de ambientes:** Los Procesos deben establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.

- **Ventana de cambios:** Los Procesos deben incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

12 POLÍTICA: REGISTRO Y AUDITORÍA

La EMPRESA DE ASEO DE PEREIRA S.A. ESP velará por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información, definiendo:

12.1 RESPONSABILIDAD

La Oficina de Control Interno será la encargada de planificar y ejecutar el seguimiento al Sistema de Gestión de Seguridad de la Información, a través de sus auditorías regulares y periódicas a los sistemas y actividades relacionadas a la gestión de activos de información.

La Oficina de Control Interno será responsable de informar los resultados de las auditorías.

12.2 ALMACENAMIENTO DE REGISTROS

El Proceso de Gestión Administrativa de la EMPRESA DE ASEO DE PEREIRA S.A. ESP velará por el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas.

Los registros de auditoría generados por la plataforma Tecnológica de los Sistemas de Información deben incluir toda la información registro y monitoreo de eventos de seguridad.

12.3 NORMATIVIDAD

La EMPRESA DE ASEO DE PEREIRA S.A. ESP velará por que las auditorías sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.

12.4 GARANTÍA CUMPLIMIENTO

La EMPRESA DE ASEO DE PEREIRA S.A. ESP garantizará la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como solucionar las deficiencias detectadas.

12.5 PERIODICIDAD

La EMPRESA DE ASEO DE PEREIRA S.A. ESP realizará la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logrará a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

13 POLÍTICA: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La EMPRESA DE ASEO DE PEREIRA S.A. ESP promoverá entre los funcionarios, empleados, contratistas de prestación de servicios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

Es responsabilidad de los funcionarios, empleados, contratistas de prestación de servicios y personal provisto por terceras partes el reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible. En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, deben notificarlo al proceso Administrativo para que se registre y se le dé el trámite necesario.

LA EMPRESA DE ASEO DE PEREIRA S.A. ESP realizará monitoreo permanente del uso que dan los funcionarios, empleados, contratistas de prestación de servicios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas físicos e informáticos de información. Además, velará por la custodia de los registros de auditoría cumpliendo con los periodos de retención establecidos para dichos registros.

El Proceso de Gestión Administrativa definirá la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales de la EMPRESA DE ASEO DE PEREIRA S.A. ESP el grupo de revisión de logs mensualmente se reunirá a analizar los resultados del monitoreo efectuado.

El Proceso de Gestión Administrativa, desarrollará y normalizará el proceso para la gestión de los incidentes de seguridad de la información, con los protocolos y formatos requeridos. De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando al Comité de Seguridad de la Información los incidentes de acuerdo con su criticidad.

El Comité de Seguridad 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

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.

14 POLÍTICA: CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El Proceso de Gestión Administrativa debe convocar a los funcionarios, empleados y contratistas a las charlas y eventos programados como parte del programa de formación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada

Los funcionarios, empleados, contratistas de prestación de servicios y personal provisto por terceras partes que por sus funciones o actividades hagan uso de la información de la EMPRESA DE ASEO DE PEREIRA S.A. ESP, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

15 FORMATOS, PROTOCOLOS Y PROCEDIMIENTOS PARA EL CUMPLIMIENTO DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

PROCEDIMIENTO
PROCEDIMIENTO PARA LA ELIMINACIÓN, RETIRO, TRASLADO O REUSO DE ACTIVOS DE INFORMACIÓN
CONTROL DE ACCESO A REDES, APLICACIONES Y/O SISTEMAS DE INFORMACIÓN
PROCEDIMIENTO DE ASIGNACIÓN, MODIFICACIÓN, REVISIÓN O REVOCACIÓN DE DERECHOS Y/O PRIVILEGIOS DE LOS USUARIOS DE LA PLATAFORMA TIC
PROCEDIMIENTO PARA LOS SERVICIOS DE INTERCAMBIO ELECTRÓNICO DE INFORMACIÓN CON GARANTÍA DE NO REPUDIO
PROCEDIMIENTO PARA EL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES
PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

PROTOCOLO
PROTOCOLO DE ENTREGA DE INFORMACIÓN EN MEDIOS REMOVIBLES
PROTOCOLO PARA USO DE SERVICIOS MÓVILES EN LA INTRANET
PROTOCOLO DE AUTORIZACIÓN DE ACCESOS A ÁREAS CON PERÍMETRO DE SEGURIDAD
PROTOCOLO DE ACUERDO DE CONFIDENCIALIDAD Y PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

FORMATO	TIPO
INVENTARIO DE ACTIVOS DE INFORMACIÓN	Registro Digital
ENTREGA DE ACTIVOS DE INFORMACIÓN A CONTRATISTAS	Registro Físico
ACUERDO DE CONFIDENCIALIDAD Y PROTECCIÓN DE ACTIVOS DE INFORMACIÓN	Registro Físico
DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN POR PARTE DE CONTRATISTAS	Registro Físico
REGISTRO E INGRESO DE DISPOSITIVOS MÓVILES A LA INTRANET	Registro Físico