AUTHENOLOGY
FIRMA ELECTRÓNICA

PSC AUTHENTICSING

Política de documentación y gestión documental.

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 20:06:39 -04'00'

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Política de documentación y gestión documental		
Tipo de Documento	Documentación sobre la Infraestructura de Clave Pública		
ID	DPO-004		
Autor	Ing. Carlos García.		
Colaboradores			
Revisado por	Samuel Gómez.	**Fecha de creación**	2024 Enero
Aprobado por	Abog. Zolangel González.	**Fecha Aprobación**	29/02/2024
Versión/Edición	1.0v	**Nº Total de Páginas**	**- 20 -**
Tipo de Uso	**Uso Interno** ☒ **Uso Público** ☐		

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Ing. Farewell Beatriz Hernández González – Cargo. Auditor Teléfono 0412-7214122 Email fhernandez@authenology.com.ve
Ing. Carlos Vicente García Gómez – Cargo. Coordinador de la Infraestructura de la Clave Pública Teléfono 0412-6049988 Email cvgcvg@gmail.com
Lic. Detriana Barrios A. – Cargo. Coordinador de Seguridad de la Información y Plataforma Teléfono 0424-218-31-97 Email detrianab@gmail.com
M.Sc. Elvis R, Chourio M. - Cargo Coordinador de Plataforma y Soporte a Usuarios Teléfono 04146017005 Email Echurio@gmail.com

ÍNDICE

1. CONTROL DE VERSIONES.

Control de Cambio			
Versión	**Revisión**	**Fecha**	**Observaciones**
1	0	30/10/2023	Versión inicial

2. TÍTULO.

Política de documentación y gestión documental

3. CÓDIGO DEL DOCUMENTO.

ID: DPO-004

4. INTRODUCCIÓN.

La presente documentación hace referencia a **AUTHENTICSING C.A**., y a su marca comercial AUTHENOLOGY, como una empresa de PSC "Proveedor de Servicios de Certificación" registrado, acreditado y autorizado por **SUSCERTE** para tal fin.

Como parte de sus procesos y funciones presenta el siguiente documento de la ***"Política de documentación y gestión documental" "DOP-004"*** esto con la finalidad de presentar, orientar, documentar y establecer las especificaciones de los requisitos para cada uno de los procesos empleados por la AC del PSC AUTHENTICSING para la generación, publicación y administración de los certificados electrónicos emitidos por **AUTHENTICSING**, y de esta manera ofrecer una mejor y sencilla comprensión e entendimiento por parte de la Junta directiva, Clientes, Proveedores, Personal y otros interesados en **AUTHENTICSING**.

5. OBJETIVO.

El presente documento tiene por objetivo presentar la "Política de documentación

y gestión documental" establecidas por el PSC **AUTHENTICSING C.A**., con las condiciones y características para emitir, gestionar, revocar y renovar los certificados electrónicos.

6. ALCANCE.

El siguiente documento de "Política de documentación y gestión documental" tiene como alcance orientar a las autoridades, clientes, sobre los procesos para generación, emisión de los diferentes certificados que serán generados y emitidos por **AUTHENTICSING C.A**, definir la autoridad de certificación y la autoridad de registro, el modelo de confianza, así como los diferentes tipos de certificados que serán emitidos por **AUTHENTICSING C.A.**

7. TÉRMINOS Y DEFINICIONES.

A los efectos de este documento se aplican las siguientes definiciones:

- **Authenology:** Se define como la marca y es el signo distintivo de la empresa **AUTHENTICSING C.A**. Su función es la de diferenciar e individualizar en el mercado unos productos o servicios de otros productos o servicios idénticos o similares, así como identificar su origen empresarial y, en cierta manera, ser un indicador de calidad y un medio de promoción de ventas.

- **Autoridad de Certificación (AC):** Significa una autoridad en la cual confían los clientes para crear, emitir y manejar el ciclo de vida de los certificados, la cual a los efectos del decreto ley de mensajes de datos y firmas electrónicas debe contar con la acreditación otorgada por SUSCERTE.

- **Autoridad de Registro (AR):** Significa la entidad cuyo propósito es suministrar apoyo local a la infraestructura de clave pública (ICP) de una Autoridad de Certificación (AC). La Autoridad de Registro desempeña un conjunto de funciones orientadas a la validación, comprobación y conformación de la documentación suministrada, así como la identidad física de un cliente que opte a la compra de una firma electrónica o certificado electrónico generado por el PSC AUTHENTICSING C.A.

- **Certificado:** Significa una estructura de datos que utiliza el estándar CCITT ITU X.509, que contiene la clave pública de una entidad junto a información asociada y presentada como "un-forgettable" (inolvidable), mediante una firma electrónica de la autoridad de certificación que la generó.

- **Cliente:** Es la entidad que ha solicitado la emisión de un certificado dentro de la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING C.A. A los

fines del Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento el Cliente será entendido como el Signatario y viceversa.

- **Firma Electrónica:** Es el dato añadido o una transformación criptográfica de una unidad de dato que permite al receptor de la unidad de dato probar la fuente y la integridad del dato y protegerse contra falsificaciones, por ejemplo, del destinatario.

- **Infraestructura de clave pública (ICP):** Es la infraestructura necesaria que genera, distribuye, maneja y archiva claves, certificados y listas de revocación de certificado de protocolo para la condición del certificado en-línea (PECL).

- **Lista de Certificados Revocados (LCR):** Significa la lista de certificados que han sido revocados o suspendidos por el PSC AUTHENTICSING C.A.

- **Alta Dirección:** Son los responsables de establecer la estrategia y los objetivos de la organización, y de garantizar que se cumplan. También son responsables de la gestión de los recursos de la organización, como el personal, el capital y los activos.

- **Norma:** Regla de comportamiento dictada por una autoridad competente que se debe seguir o a la que se deben ajustar las conductas, tareas, actividades, etc.

- **Procedimiento:** Acciones que se realizan, con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo. Se distinguen dos clases de procedimientos: obligatorios y recomendados. Estos últimos representan “buenas prácticas”, que son aconsejables, pero no requeridas. Si en un procedimiento no se utiliza la palabra “recomendado” se asume que es obligatorio.

- **Protocolo de Estatus de Certificado En-línea (Online Certificate Status Protocol)**: Es un protocolo utilizado para validar el estado de un certificado en tiempo real. La respuesta de las solicitudes incluye tres estados: valido, revocado o desconocido. Su definición en Idioma Inglés es OCSP (Online Certificate Status Protocol).

- **Proveedor:** Es una organización o persona que suministra un producto o servicio para los PSC (Proveedor de Servicios de certificación)

- **PSC:** Proveedor de Servicios de Certificación

- **Registro:** Conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos, informatizada o no. A los efectos de esta Política se clasifican en:
  - **Registros de Funcionamiento**: Son los asociados con las actividades de

soporte a las actividades principales (Directores, Gerentes y Personal Técnico) de PSC AUTHENTICSING.

- ❖ **Registros Personales:** Son los relacionados con las personas físicas o jurídicas.
- ❖ **Registros de Producción:** Son los asociados a las actividades de Authenticsing o de alguno de sus miembros.

- ➢ **Registro de Auditoría:** Es la unidad de dato discreta para el rastro de auditoría cuando ocurre un evento que es examinado y registrado. Un registro de auditoría consiste de un conjunto de descripciones de auditoría, cada uno de los cuales tiene un conjunto de atributos de auditoría asociados a éste. Cada registro de auditoría tiene una descripción de auditora para el encabezamiento del registro y usualmente tiene descripciones de auditoría adicionales que describen la entidad(es) y objeto(s) involucrados en el evento.

- ➢ **Responsable del Área de Recursos Humanos:** Director General de Personal dependiente del departamento de RRHH.

- ➢ **Seguridad de la Información:** La seguridad de la información se entiende como la preservación de las siguientes características:
  - ❖ **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
  - ❖ **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
  - ❖ **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- ❖ **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- ➢ **Servicios de Certificación**: Son los servicios que pueden proporcionar con respecto al manejo del ciclo de vida de un certificado para cualquier tipo de nivel de jerarquía de la ICP, esto incluye servicios auxiliares, tales como; servicios OCPS, servicios de tiempo compartido, servicios de verificación de identidad, hospedaje de lista de certificados revocados (LCR), etc.

- **Validación:** Es un proceso que lleva a cabo la verificación de validez de un Certificado en términos de su estatus o condición (Ej. si es suspendido o revocado).

8. POLÍTICA DE GESTIÓN DOCUMENTAL

El PSC Authenticsing adopta este documento para fijar políticas y reconoce la importancia de los documentos recibidos y preparados de acuerdo con sus términos, utilizando las tareas como insumo para la toma de decisiones con una planificación adecuada.

Gestionar documentos para mantener su integridad, autenticidad, precisión y la exactitud de los parámetros técnicos de organización, seguridad, conservación y destrucción, acceso más fácil a los documentos, prioridad de la transparencia de las operaciones gestión y conservación de cada uno de los patrimonio documental.

Las políticas de gestión documental promueven políticas y fortalezas de calidad. Creando así un mecanismo de participación y confianza entre la ciudadanía, el estado y el gobierno, mejorando procesos y continuar en constate mejora.

Por tanto, los lineamientos y objetivos generales de la Política de Gestión documental del PSC Authenticsing son las siguientes:

- Garantizar que todos los documentos relevantes estén actualizados y disponibles para los empleados y los clientes.
- Proteger la confidencialidad, la integridad y la disponibilidad de los documentos.
- Facilitar el acceso a los documentos por parte de los empleados y los clientes
- Mejorar la eficiencia de los procesos de negocio mediante la automatización de la documentación y gestión documental.
- El modelo de archivo tiene en cuenta el ciclo de vida del documento y sus pautas de procedencia archivados y de pedido original.
- Determinar las responsabilidades que debe asumir cada institución en relación con la creación, organización (clasificación, ordenación y descripción) y almacenamiento de documentos y archivos durante su ciclo de

vida.

- Asignar presupuesto y personal para organizar y preservar archivos.
- Adoptar las acciones necesarias para asegurar el almacenamiento a largo plazo de los documentos de archivo electrónico en los distintos sistemas de información y bases de datos de la unidad estructural, e implementar una serie de acciones y normas relacionadas con los documentos bajo su control. El medio y método de grabación o almacenamiento para asegurar su conservación a largo plazo, independientemente de la etapa de su ciclo de vida.
- Intentar seguir los principios de los procesos de gestión de documentos.
- Organizar archivos de acuerdo con estándares técnicos y capacitación de los empleados.
- Asegúrese de que los documentos se conserven y estén organizados adecuadamente para que puedan buscarse en cualquier medio en el que se encuentren.

9. RESPONSABILIDADES.

9.1 La Alta Dirección es responsable de

- Aprobar la política de documentación y gestión documental.
- Asegurar que la política se implemente y mantenga de manera efectiva.
- Proveer los recursos necesarios para la implementación y el mantenimiento de la política.

9.2 El Gerente de Documentación y Gestión Documental es responsable de

- Implementar y mantener la política de documentación y gestión documental.
- Desarrollar y mantener los procesos y procedimientos para la documentación y gestión documental.
- Proveer educación y capacitación a los empleados sobre la documentación y gestión documental.

9.3 Los empleados son responsables de

- Crear, revisar, aprobar, distribuir, almacenar y eliminar documentos de acuerdo con la política.
- Proteger la confidencialidad, la integridad y la disponibilidad de los documentos.

9.4 El Gerente de Recursos Humanos

Es responsable de garantizar que los documentos de recursos humanos cumplan con las leyes y regulaciones aplicables.

10. PROCESO Y PROCEDIMIENTOS

10.1 Proceso de creación de documentos

- Identificación de la necesidad de un documento: El solicitante del documento debe identificar la necesidad de un documento.
- Desarrollo del documento: El autor del documento debe desarrollar el documento de acuerdo con los requisitos de la política de documentación y gestión documental.
- Revisión del documento: El documento debe ser revisado por un revisor independiente para garantizar que sea preciso y completo.
- Aprobación del documento: El documento debe ser aprobado por un aprobador autorizado antes de su distribución.

10.2 Proceso de revisión de documentos

- Identificación de los documentos que necesitan ser revisados: El Gerente de Documentación y Gestión Documental debe identificar los documentos que necesitan ser revisados.
- Programación de la revisión: Se debe realizar o programar la revisión de los documentos.
- Revisión de los documentos: El personal asignado debe revisar los documentos de acuerdo con los requisitos de la política de documentación y gestión documental.
- Aprobación de los cambios: Los cambios a los documentos deben ser aprobados por un aprobador autorizado.

10.3 Proceso de distribución de documentos

- Determinación de los destinatarios: Es necesario determinar los destinatarios de los documentos de Authenticsing.
- Envío de los documentos: Los documentos deben ser enviados a los destinatarios de acuerdo con los requisitos de las políticas.

10.4 Proceso de almacenamiento de documentos

- Determinación del método de almacenamiento: Se debe determinar el método de almacenamiento de los documentos.
- Almacenamiento de los documentos: Los documentos deben ser almacenados de acuerdo con los requisitos de la política de documentación y gestión documental.

10.5 Proceso de eliminación de documentos

- Determinación de los documentos que necesitan ser eliminados: Se debe determinar los documentos que necesitan ser eliminados.
- Procedimiento de eliminación: Los documentos deben ser eliminados de acuerdo con los requisitos de la política de documentación y gestión documental.

11. ARCHIVO Y RETENCIÓN

EL PSC Authenticsing establece un sistema de archivo y retención para garantizar que los documentos se conserven de manera segura y durante el período de tiempo requerido.

11.1 Directrices

- Los documentos deben ser archivados y retenidos de acuerdo con los requisitos de la política de documentación y gestión documental.
- Los documentos deben ser almacenados en un lugar seguro para protegerlos de la pérdida, la destrucción y el acceso no autorizado.
- Los documentos deben ser accesibles a los empleados y los clientes que necesitan acceder a ellos.

11.2 Proceso

- Identificación de los documentos que necesitan ser archivados y retenidos: Se deberá identificar los documentos que necesitan ser archivados y retenidos.
- Determinación del período de retención: Se debe determinar el período de retención para cada documento.
- Clasificación de los documentos: Los documentos deben ser clasificados según su importancia y sensibilidad.
- Almacenamiento de los documentos: Los documentos deben ser almacenados de acuerdo con su clasificación.
- Acceso a los documentos: Los documentos deben ser accesibles a los

empleados y los clientes que necesitan acceder a ellos.

- ❖ Destrucción de los documentos: Los documentos deben ser destruidos de manera segura al final del período de retención.

11.3 Tabla de Retención

Tabla de retención para especificar el período de retención para cada tipo de documento.

Tipo	Período de Retención
Políticas	Anualmente
Procedimientos	Anualmente
Registro de Auditoria	10 años
Informes de Certificación	5 años

11.4 Procedimiento de destrucción

El PSC Authenticsing ha determinado un procedimiento de destrucción para garantizar que los documentos se destruyan de manera segura al final del período de retención. El procedimiento de destrucción debe ser aprobado por la Alta Dirección.

- ❖ Los documentos deben ser triturados o eliminados por medios electrónicos.
- ❖ Los documentos triturados o eliminados deben ser inutilizables.
- ❖ El proceso de destrucción debe ser registrado.

Algunos puntos adicionales para el archivo y la retención de documentos:

- ➢ Authenticsing realiza auditorías anualmente para verificar el cumplimiento de la política de archivo y retención.
- ➢ Documentar todos los procesos y procedimientos de archivo y retención.
- ➢ Capacitar a los empleados sobre los requisitos de archivo y retención.

12. SEGURIDAD Y ACCESO

El PSC Authenticsing establece un sistema de seguridad y acceso para proteger la confidencialidad, la integridad y la disponibilidad de los documentos

12.1 Directrices

- Los documentos deben estar protegidos de la pérdida, la destrucción y el acceso no autorizado.
- Solo los empleados autorizados deben tener acceso a los documentos.
- El acceso a los documentos debe ser registrado.

12.2 Proceso

- Identificación de los riesgos de seguridad: Se debe identificar los riesgos de seguridad asociados con los documentos.
- Implementación de controles de seguridad: Se debe implementar controles de seguridad para mitigar los riesgos identificados.
- Supervisión de los controles de seguridad: Se debe supervisar los controles de seguridad para garantizar que sean efectivos.

12.3 Controles de seguridad

- Autenticación: Los empleados deben autenticarse antes de acceder a los documentos.
- Autorización: Los empleados solo deben tener acceso a los documentos para los que están autorizados.
- Encriptación: Los documentos confidenciales deben estar encriptados.
- Acceso restringido: El acceso a los documentos debe estar restringido a áreas seguras.
- Registro de acceso: El acceso a los documentos debe ser registrado.

12.4 Procedimiento de acceso

Un procedimiento de acceso va garantizar que solo los empleados autorizados tengan acceso a los documentos. El procedimiento de acceso debe ser aprobado por la Alta Dirección. Y se debe realizar los siguientes pasos:

- Realizar auditorías periódicas para verificar el cumplimiento de la política de seguridad y acceso.
- Documentar todos los procesos y procedimientos de seguridad y acceso.
- Capacitar a los empleados sobre los requisitos de seguridad y acceso.
- Se debe verificar la autorización del empleado para acceder a los documentos.

13. CONTROL DE CAMBIOS

Un sistema de control de cambios garantiza que los cambios a los documentos de Authenticsing se realicen de manera controlada y documentada.

13.1 Directrices

- Los cambios a los documentos deben ser aprobados por un personal autorizado.
- Los cambios a los documentos deben ser registrados.
- Los cambios a los documentos deben ser comunicados a los usuarios afectados.

13.2 Proceso

- Solicitud de cambio: El solicitante del cambio debe completar un formulario de solicitud de cambio.
- Evaluación de cambio: Se deberá evaluar la solicitud de cambio.
- Aprobación de cambio: La solicitud de cambio debe ser aprobada por un personal autorizado.
- Implementación de cambio: El cambio debe ser implementado por el autor del documento.
- Comunicación de cambio: Los usuarios afectados deben ser notificados del cambio.

13.3 Formulario de solicitud de cambio

El formulario de solicitud de cambio debe incluir los siguientes campos:

- Nombre del documento: El nombre del documento que se va a cambiar.
- Descripción del cambio: Una descripción detallada del cambio solicitado.
- Razón del cambio: La razón por la que se solicita el cambio.
- Impacto del cambio: El impacto del cambio en los usuarios del documento.
- Aprobador autorizado: El nombre del aprobador autorizado que debe aprobar el cambio.

13.4 Procedimiento de aprobación de cambios

El procedimiento de aprobación de cambios debe ser aprobado por la Alta Dirección. El Control de cambio debe contener lo siguiente:

- Nombre del documento: El nombre del documento que se ha cambiado.
- Fecha del cambio: La fecha en que se realizó el cambio.

- ❖ Descripción del cambio: Una descripción detallada del cambio realizado.
- ❖ Aprobador autorizado: El nombre del aprobador autorizado que aprobó el cambio.

13.5 Comunicación de cambios:

La comunicación de cambios debe incluir los siguientes elementos:

- ❖ Una descripción del cambio que se ha realizado.
- ❖ La fecha en que el cambio entrará en vigor.
- ❖ Especificación de cómo el cambio afectará a los usuarios.

De esta manera los cambios a los documentos estarán de forma controlada y documentada

14. CAPACITACIÓN

14.1 Directrices:

- ➢ La educación y capacitación debe ser proporcionada a todos los empleados que crean, utilizan o mantienen documentos de Authenticsing.
- ➢ La educación y capacitación debe ser apropiada para el nivel de responsabilidad del empleado.
- ➢ La educación y capacitación debe ser actualizada periódicamente para reflejar los cambios en los requisitos.

14.2 Proceso

- ➢ Identificación de las necesidades de educación y capacitación: Se deberá identificar las necesidades de educación y capacitación de los empleados.
- ➢ Desarrollo de un plan de educación y capacitación: Se debe desarrollar un plan de educación y capacitación para satisfacer las necesidades identificadas.
- ➢ Implementación del plan de educación y capacitación: El plan de educación y capacitación debe ser implementado.
- ➢ Evaluación de la eficacia de la educación y capacitación: La eficacia de la educación y capacitación debe ser evaluada.

14.3 Métodos capacitación

Authenticsing utiliza métodos de educación y capacitación para satisfacer las necesidades de los empleados. Algunos métodos comunes incluyen:

- ❖ Clases presenciales: Las clases presenciales son una forma efectiva de

proporcionar capacitación a un grupo de personas.

- E-learning: El e-learning es una forma eficaz de proporcionar capacitación a los empleados de forma remota.
- Tutoría: La tutoría es una forma eficaz de proporcionar capacitación a los empleados de forma individualizada.

14.4 Contenido capacitación

El contenido de la educación y capacitación debe cubrir los siguientes temas:

- Los requisitos de documentación y gestión documental del PSC Authenticsing.
- Los procesos y procedimientos de documentación y gestión documental.
- Las herramientas y tecnologías utilizadas para la documentación y gestión documental.

14.5 Evaluación de la eficacia de capacitación

Algunos métodos comunes de evaluación que se incluyen son:

- Exámenes: Los exámenes son una forma eficaz de evaluar el conocimiento de los empleados.
- Actividades prácticas: Las actividades prácticas son una forma eficaz de evaluar las habilidades de los empleados.
- Realimentación de los empleados: La realimentación de los empleados es una forma eficaz de obtener información sobre la eficacia de la capacitación.

Al implementar un programa de educación y capacitación eficaz, el PSC Authenticsing puede garantizar que los empleados tengan los conocimientos y habilidades necesarios para crear, utilizar y mantener lo asignado para cada personal y que se cumpla de manera eficaz.

15. AJUSTES AL DOCUMENTO.

Los ajustes a la documentación requerida por SUSCERTE para la operación de un PSC, serán realizados en cada oportunidad que ocurra un cambio en el marco normativo y legal aplicable a los PSC, cuando suceda un cambio técnico que justifique el ajuste o cambio, cuando sea requerido y solicitado por SUSCERTE o en su revisión anual.

15.1 Mecanismo de desarrollo del documento:

El presente documento de la política de documentación y gestión documental se encuentra desarrollado sobre la base de la normativa de acreditación aplicable a los interesados a convertirse en PSC. Dicha norma de acreditación es dictada y emitida por SUSCERTE.

15.2 Mecanismo para ajuste del documento:

Los cambios en el decreto ley de mensajes de datos y firmas electrónicas, su reglamento, la normativa de SUSCERTE o de la norma internacional vinculante y exigida para la operación de los PSC, que contemplen cambios sustanciales en los procesos y métodos de seguridad y operación, los cuales incluyan variación de los procedimientos y actividades de los PSC producirán una revisión del presente Documento, con el objetivo de ajustar los procesos y procedimientos a los estándares y normativa aplicable y validadas por SUSCERTE para la operación de los PSC.

Todo ajuste al presente documento de la Política de documentación y gestión documental, será producto del trabajo del personal técnico y legal del PSC AUTHENTICSING y exigirá contar para su implementación, con la aprobación y validación de alta dirección, de acuerdo a lo descrito en el punto de "Mecanismo para aprobación de los ajustes al documento" del presente documento. El proceso llevado a cabo para el ajuste será documentado y realizado conforme al documento de la política de documentación y gestión documental.

15.3 Mecanismo para aprobación de los ajustes al documento:

Cada ajuste o modificación del documento de la política de documentación y gestión documental tendrá que contar con la aprobación de la alta dirección del PSC AUTHENTICSING, ser documentada y constar por escrito, nombrando el número de edición y revisión, fecha de elaboración, fecha de aprobación y la firma del representante de la alta dirección que aprueba el ajuste o modificación.

Se documentará el ajuste o modificación y su aprobación conforme al documento de la política de documentación y gestión documental.

16. MARCO LEGAL Y NORMATIVO.

- Decreto ley de mensaje de datos y firmas electrónicas y su reglamento.
- Normativa de la Superintendencia de Servicios de Certificación Electrónica
- (SUSCERTE).
- Normativa AUTHENTICSING.
- Estándar internacional ITU- T X.509 V3.

- Estándar Internacional ITU-T X.609.
- Norma ISO 9000:2015.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2001.
- Norma ISO/IEC 27001:2013.

--- Fin de Documento ---