AUTHENOLOGY
FIRMA ELECTRÓNICA

AUTHENTICSING C.A

Política de Seguridad de la Información.

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 20:02:49 -04'00'

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Política de seguridad de la información.		
Tipo de Documento	Documentación Técnica sobre las Políticas		
ID	DPO-003		
Autor	Ing. Carlos García.		
Colaboradores			
Revisado por	Samuel Gómez.	**Fecha de creación**	2024 Enero
Aprobado por	Abog. Zolange González.	**Fecha Aprobación**	29/02/2024
Versión/Edición	1.0v	**Nº Total de Páginas**	**- 42 -**
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

Índice 3
1. CONTROL DE VERSIONES. 6
2. TÍTULO. 6
3. CÓDIGO DEL DOCUMENTO 6
4. INTRODUCCIÓN. 6
5. OBJETIVO. 7
6. ALCANCE. 7
7. TÉRMINOS Y DEFINICIONES. 8
8. POLITICAS. 13
8.1 Objetivos. 13
8.2 Política de Seguridad de la Información. 14
8.3 Revisión de las políticas de seguridad de la información. 14
9. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD. 14
9.1 Organización Interna 15
9.1.1 Objetivos. 15
9.1.2 Funciones y responsabilidades de la seguridad de la información. 15
9.1.3 Separación de funciones. 16
9.1.4 Contacto con autoridades. 17
9.1.5 Seguridad de la información en la gestión de proyectos. 17
10. Seguridad Ligada a los Recursos Humanos 17
10.1 Previo al empleo 17
10.1.1 Selección. 17
10.1.2 Términos y condiciones de empleo. 18
10.2 Durante el empleo. 18
10.2.1 Responsabilidades de la Dirección. 18
10.2.2 Toma de conciencia, educación y formación en la seguridad de la información. 18
10.2.3 Proceso disciplinario. 19
10.3 Finalización o cambio de empleo. 19
10.3.1 Responsabilidades de terminación 19

11. GESTION DE ACTIVOS. 20
11.1 Responsabilidad por los activos. 20
11.1.1 Inventario de activos. 20
11.1.2 Propiedad de los activos 20
11.1.3 Uso aceptable de los activos 21
11.1.4 Devolución de los activos 21
11.2 Clasificación de la información. 21
11.3 Manejos de los soportes. 22
12. CONTROL DE ACCESOS. 24
12.1 Requisitos de negocio para el control de acceso 24
12.1.1 Política de control de los accesos: 24
12.1.2 Acceso a las redes y a los servicios de red. 25
12.2 Gestión del Acceso de usuarios 28
12.2.1 Acceso a los usuarios. 28
12.2.2 Gestión de privilegiados. 29
12.2.3 Remoción o ajuste de los derechos de acceso. 29
13. CONTROLES CRIPTOGRÁFICOS 30
13.1 Políticas sobre el empleo de controles criptográficos. 30
13.2 Gestión de claves. 30
13.2.1 Relativas a la construcción de las contraseñas. 31
14. SEGURIDAD FÍSICA Y DEL AMBIENTE. 31
14.1 Áreas seguras 31
14.1.1 Perímetro de seguridad física. 31
14.2 Equipamiento 32
14.2.1 Ubicación y protección del equipamiento. 32
14.2.2 Seguridad del Cableado. 33
14.2.3 Mantenimiento de Equipos. 34
14.2.4 Seguridad en la reutilización o eliminación de equipos 34
14.2.5 Política de escritorio limpio. 34
15. SEGURIDAD DE LAS OPERACIONES. 34
15.1 Documentación de Procedimientos Operativos. 35
15.2 Respaldo de la información. 35
15.3 Protección ante software malicioso. 36

15.3.1 Controles ante software malicioso....36
15.4 Respaldo de la información. 38
15.4.1 Verifique su validez 38
15.4.2 Medios de recuperación 39
15.4.3 Mantener registros....39
16. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO....39
16.1 Gestión de la continuidad del negocio. 39
16.1.1 Administración de la continuidad de la empresa. 40
16.1.2 Implementación de la continuidad de la seguridad de la información. 40
16.2 Redundancias....40
17. CUMPLIMIENTO. 41
18. REVISIÓN, APROBACIÓN Y MODIFICACIÓN. 41
19. MARCO LEGAL, NORMATIVO Y DOCUMENTACIÓN APLICABLE....41
20. FUNCIONES Y RESPONSABILIDADES....41

1. CONTROL DE VERSIONES.

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

2. TÍTULO.

Política de seguridad de la información.

3. CÓDIGO DEL DOCUMENTO

DPO-003

4. INTRODUCCIÓN.

El Proveedor de Servicios de Certificación (PSC) “AUTHENTICSING”, en su carácter de empresa de PSC y como parte de sus procesos y funciones presenta el siguiente documento “Políticas de la Seguridad de la Información” cuya finalidad es documentar e informar a todos sus clientes, signatarios, proveedores, aliados comerciales y demás partes interesadas de la AC y AR de AUTHENTICSING, con respecto a la función y uso de las Políticas de la Seguridad de la Información implementadas dentro de los procesos y funciones de generación de firmas y certificados electrónicos así como de nuestra plataforma tecnológica, a los fines de cumplir con los requerimientos de las normas y políticas de seguridad.

Para **AUTHENTICSING** comprometido con la seguridad y el resguardo de la información como un activo de gran importancia el cual valoramos y por el cual debemos asegurar la información de nuestros clientes y signatarios para la correcta administración de la seguridad de la información.

La política de seguridad es un documento de alto nivel que denota el compromiso de **AUTHENTICSING** con la seguridad de la información, las políticas de seguridad de información son esencialmente las orientaciones e instrucciones que indican los

procesos para proceder los asuntos de seguridad en **AUTHENTICSING** el cual forman las bases para la implementación de las medidas de seguridad y protección de la información en **AUTHENTICSING,** estas políticas van acompañadas de normas, instrucciones, procedimientos y técnicas destinadas a conseguir y mantener nuestra plataforma tecnológica y mantener nuestro sistema de información seguro y confiable. En **AUTHENTICSING** implementamos las políticas de seguridad que buscan proteger la integridad de información esto con el fin de minimizar las amenazas y riesgo que se puedan afectar la continuidad de los procesos del sistema, es por eso que para la correcta administración de la Seguridad de la Información en **AUTHENTICSING** se ha establecido un conjunto de normas y programas que buscan cumplir con los requerimientos de mayor importancia como son:

Confidencialidad: La confidencialidad, es un principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.

Integridad: Este término, en seguridad informática, se puede definir como la garantía de exactitud y fiabilidad de la información. Asegurando la integridad de la información y los datos se consigue prevenir cualquier modificación no autorizada de esta.

Disponibilidad: La disponibilidad supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados.

5. OBJETIVO.

El presente documento “Políticas de Seguridad de la Información” tiene como objetivo mostrar e informar a los usuarios el proceso, normas, instrucciones, procedimientos y directrices para establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte de la plataforma de **AUTHENTICSING.**

6. ALCANCE.

Las políticas de Seguridad de la Información son aplicables para todo **AUTHENTICSING,** sus clientes, signatarios, aliados comerciales, proveedores que deberá cumplir con las más mínimos requisitos con el fin de garantizar la adopción del conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información.

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.
- **Activos de Información:** Son los bienes relacionados a un sistema de información en cualquiera de sus etapas. Ejemplos de activos son:
  - Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, etc.
  - Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.
  - Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.
- **Administración de Riesgos:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Aplicación:** Se refiere a un sistema informático, tanto desarrollado por AUTHENTICSING como por terceros, o al sistema operativo o software de base, que integren los sistemas de información o donde estos estén alojados.
- **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:** 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 AUTHENTICSING
- **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.
- **Cifrado:** Significa el proceso mediante el cual los datos simples de un texto son

transformados para ocultar su significado. El cifrado es un proceso reversible que se efectúa mediante el uso de un algoritmo criptográfico y una clave.

- **Clave Asimétrico:** Es el par de claves relacionadas, en el cual la clave privada define la modificaciones privada y la clave pública define la transformación pública.
- **Cliente:** Es la entidad que ha solicitado la emisión de un certificado dentro de la Infraestructura de Clave Pública (ICP) del AUTHENTICSING**.** 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.
- **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. En AUTHENTICSING esta función es cumplida por la Comisión de Seguridad de la Información. Dentro de esta Política los términos Comité de Seguridad de la Información y Comisión de Seguridad de la Información son considerados equivalentes.
- **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de AUTHENTICSING**.**
- **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.
- **Generación de Certificado:** Proceso de crear un certificado a partir de datos de entrada que son específicos a la aplicación y al cliente.
- **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
- **Información de Identificación:** Es cuando se obtiene una información para identificar positivamente a una entidad y suministrarle los servicios de certificación que solicite.
- **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).
- **Infraestructura Operacional:** Es la Infraestructura tecnológica mediante la cual se suministran los servicios de certificación.
- **Integridad de Datos:** Es la condición de ser preciso, completo y válido de no ser alterado o destruido de manera no autorizada.
- **Lista de Certificados Revocados (LCR):** Significa la lista de certificados que

han sido revocados o suspendidos por el AUTHENTICSING**.**

- **Manejo de Clave:** Es la administración y el uso de la generación, inscripción, certificación, la desincorporación, distribución, instalación, almacenamiento, archivo, revocación, derivación y destrucción del material de clave de acuerdo con la política de seguridad.
- **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.
- **Par Clave:** Son las claves de un sistema criptográfico asimétrico, y que tienen como función que uno de los pares de claves descifrará lo que el otro par de clave cifra.
- **Par de claves asimétrico:** Significa el par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.
- **Parte interesada:** Significa la organización o persona que tiene interés en el desempeño o éxito del AUTHENTICSING
- **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.
- **Proceso de Información:** Conjunto de tareas relacionadas lógicamente que se realizan para lograr un resultado determinado en un Sistema de Información.
- **Proceso de Verificación:** Es todo proceso que toma como entrada de datos un mensaje firmado, la clave de verificación y los parámetros de dominio que arroja como salida el resultado de verificación de la firma, si es válida o inválida.
- **Propietario de un Activo Físico:** Es el responsable patrimonial del bien.
- **Propietario de un Proceso de Información:** Es el responsable por la creación, puesta en funcionamiento y mantenimiento de un proceso de Información.
- **Propietarios de la Información:** Son los funcionarios, unidades académicas o dependencias responsables de la generación o recopilación de la información, con competencia jurídica para administrar y disponer de su contenido.
- **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 AUTHENTICSING PSC.
- ❖ 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 de la Unidad de Auditoría Interna**: Auditor Interno Titular.
- ➢ **Responsable de la Unidad Organizativa:** Director o Gerente General, Secretario, Gerente de unidad o Director responsable del funcionamiento de la Unidad Organizativa.
- ➢ **Responsable del Área Informática:** Director del departamento de Informática.
- ➢ **Responsable de una Aplicación:** Encargado de la instalación y mantenimiento de la aplicación.
- ➢ **Responsable del Área Legal:** Director de Asuntos Jurídicos.
- ➢ **Responsable del Área de Recursos Humanos:** Director General de Personal dependiente del departamento de RRHH.
- ➢ **Responsable de Seguridad Informática:** Director del departamento de Informática.
- ➢ **Responsable de un Sistema de Información:** Encargado de velar por la puesta en marcha y el correcto funcionamiento del Sistema de Información o en su defecto el Responsable de la Unidad Organizativa.
- ➢ **Revocación:** Es el cambio de estatus de un certificado válido o suspendido a "revocado" a partir de una fecha específica en adelante.
- ➢ **Revocación de Certificado:** Son los procesos que consisten en cambiar el estatus de un certificado válido o suspendido o revocado. Cuando un certificado tiene un estado revocado, esto significa que una entidad ya no es confiable para ningún objetivo.
- ➢ **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.

Adicionalmente, deberán considerarse los conceptos de:

- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la AUTHENTICSING.
- Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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.
- Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- Tecnología de la Información: La tecnología de la información (TI) es el proceso de creación, almacenamiento, transmisión y percepción de la información y los métodos de aplicación de dichos procesos.

- **Seguridad Física:** Es la medida utilizada para proveer protección física a los recursos contra amenazas intencionales y accidentales.
- **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.
- **Sociedad Mercantil o Sociedad de Capital:** Persona jurídica que se crea para iniciar una actividad comercial con fines de lucro. En este sentido, se agrupan una o más personas físicas o morales, según la legislación mercantil, convirtiéndose ahora en socios para desempeñar una actividad económica.
- **Solicitante**: La persona física o jurídica que solicita (o pretende renovar) un Certificado. Una vez que se emite el Certificado, el Solicitante se denomina Suscriptor. Para los Certificados emitidos a dispositivos, el Solicitante es la entidad que controla u opera el dispositivo mencionado en el Certificado, incluso si el dispositivo envía la solicitud de certificado real.
- **Solicitud de Certificado:** Es la solicitud autenticada de una entidad por su autoridad matriz para emitir un certificado que une la identidad de esa entidad a una clave pública.
- **Unidades Organizativas:** Las Unidades Organizativas de **AUTHENTICSING PSC.** son las Unidades y las áreas de la administración central que dependen directamente del Director o Gerente General. Las Unidades Organizativas se detallarán en la estructura organizativa de la empresa.
- **Uso del Certificado:** Conjunto de reglas que indican la aplicabilidad del certificado de una comunidad en particular y/o la clase de aplicación con requerimientos de seguridad comunes.
- **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. POLITICAS.

Las políticas de seguridad de la información consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. Esta política de seguridad establece todos los requisitos mínimos para asegurar la continuidad de las operaciones.

8.1 Objetivos.

En la política de seguridad de la información de AUTHENTICSING proporciona una orientación y apoyo de la dirección para la seguridad de la información, de

acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes establecida. La implementación de estas políticas se basa en el esfuerzo que requiere de la participación de todos los empleados, personal técnico, profesional, directores y aliados comerciales de AUTHENTICSING que trabajan con activos de información.

Es políticas y obligación de AUTHENTICSING, el seguimiento cabal del conjunto de normas para crear, emitir, mantener, actualizar y publicar las acciones y procedimientos orientados a cumplir con las normas, leyes, reglamento requerido por la SUSCERTE y las normativas internacionales para el aseguramiento de las actividades y operaciones relacionadas a la Seguridad de la Información.

8.2 Política de Seguridad de la Información.

Esta Política se conforma por una serie de pautas sobre aspectos específicos de la Seguridad de la Información, es por esto que la comunicación de las políticas debe realizarse a todos los niveles, no solo al nivel de los directivos y responsables, el cual involucrar a toda la organización en esta tarea.

8.3 Revisión de las políticas de seguridad de la información.

Las políticas de la Seguridad de la información debe ser revisado al menos una vez al año o cuando surjan cambios relevantes de mejora y de cumplimiento de Seguridad de la Información en Authenticsing, SUSCERTE o de algún cambio o ajuste de las normas internacional; por lo que no deben permanecer estáticas por largo tiempo.

Se trata entonces de mantener actualizada la política de la seguridad de la información. Para ello es interesante tener en cuenta algunas recomendaciones:

- Una política general de la alta dirección para expresar el compromiso de toda Authenticsing con la seguridad de la información.
- Otras políticas definidas por las direcciones y/o áreas de la Authenticsing.
- Instrucciones técnicas o documentos de aplicabilidad de las políticas definidas en las políticas específicas de Authenticsing.

9. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD.

Orientado para implementar y administrar la Seguridad de la Información dentro de AUTHENTICSING, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener

responsabilidades bien definidas y proteger las informaciones de carácter confidencial

9.1 Organización Interna

9.1.1 Objetivos.

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

9.1.2 Funciones y responsabilidades de la seguridad de la información.

9.1.2.1 El Comité de Seguridad y riesgo.

Los miembros de la comisión están conformados principalmente por los siguientes:

- Alta Gerencia: Conformada por la Junta directiva de Authenticsing y representado por uno de los directores de la alta dirección.
- Gerente General: Representada por el gerente general de Authenticsing.
- Coordinador de seguridad de la información y plataforma tecnológica: Representado por el personal asignado para este cargo.
- Consultor de seguridad: Consultor Interno y Consultor Externo.
- Responsabilidades del comité de seguridad de la información serán las siguientes:
  - Revisar y proponer a la alta gerencia de Authenticsing para su aprobación, la política y las funciones generales en materia de seguridad de la información.
  - Elaborar, promover y mantener la política de seguridad de la información.
  - Elaborar el plan de riesgos y las posibles soluciones para mitigar las amenazas.
  - Proponer nuevos objetivos en materia de seguridad de la información.
  - Desarrollar y mantener el marco normativo de seguridad y controlar su cumplimiento.
  - Validar la implantación de los requisitos de seguridad necesarios.
  - Liderar la implantación del SGSI.
  - Establecer los controles y medidas técnicas y organizativas para asegurar los sistemas de información.
  - Gestionar la seguridad de la información de la organización de manera global.
  - Gestionar y analizar las incidencias de seguridad que tienen lugar

en la organización.

- ❖ Revisar periódicamente el estado de la seguridad de la información.
- ❖ Realizar el seguimiento de los incidentes de seguridad.
- ❖ Controlar y revisar los indicadores definidos.
- ❖ Controlar que las auditorías de seguridad se realicen con la frecuencia necesaria.
- ❖ Revisar los informes de auditoría.
- ❖ Definir y comprobar la aplicación del procedimiento de copias de respaldo y recuperación de datos.
- ❖ Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidencias.
- ❖ Reportar al Comité de Seguridad las cuestiones relevantes en materia de seguridad de la información
- ❖ Asegurar que las metas de la seguridad de información estén identificadas, relacionadas con las exigencias organizacionales, operativas y funcionales del negocio.

9.1.3 Separación de funciones.

Todo el personal que tenga acceso a la información de Authenticsing debe tener claramente definidos sus deberes frente a la gestión de la Seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.

En todos los sistemas de información de Authenticsing se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- ➢ Cumplir la normativa nacional aplicable en la materia, en particular con lo establecido por el decreto Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento, normativas de SUSCERTE
- ➢ Cumplir con las políticas de seguridad de la información, así como con los procedimientos que se desprendan de estas, independientemente del cargo que desempeñe y de la naturaleza del vínculo con Authenticsing.
- ➢ Reportar los eventos o incidentes de seguridad de la información que detecte al responsable de Seguridad de la Información y/o comité de seguridad.
- ➢ Proteger y resguardar toda la información confidencial, reservada o restringida para el negocio de la Administración, sean estos informes,

datos, proyecciones, métodos, estrategias u otros en el cumplimiento de los objetivos estratégicos.

- Participar de las actividades de capacitación y concientización en seguridad de la información que Authenticsing determine.

9.1.4 Contacto con autoridades.

Authenticsing contara con procedimiento que especifiquen cuando y cuales autoridades contactar en caso de que se sospeche de la violación de la Ley o normas o de incidentes relacionados con el área.

9.1.5 Seguridad de la información en la gestión de proyectos.

La seguridad de la información se debe integrar al procedimiento de gestión de proyectos de Authenticsing, esto con la finalidad de asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de proceso, de los funcionarios y contratistas de la OTI, asegurar que se sigan las siguientes directrices:

- Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.
- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

10. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

La implementación de controles de selección, de Recursos Humanos adecuados y proporcionales, en todas las etapas de selección de nuevos empleados, reduce las amenazas accidentales o maliciosas. Esto es válido para empleados como para contratistas.

- Objetivo

Asegurar que los empleados, contratista y usuarios de terceras partes comprendan sus responsabilidades, que sean apropiadas para los roles considerados y así reducir el riesgo de hurto, fraude y de los recursos.

10.1 Previo al empleo

10.1.1 Selección.

Se deberá realizar la revisión y verificación de antecedentes de los

candidatos, en concordancia con las regulaciones de las leyes, regulaciones y ética pertinentes; y debe ser proporcional a la confidencialidad de la información que tendrá que conocer el empleado. Se verificaran:

- Certificados de títulos académicos y profesionales
- Chequeo de referencia laborales y personales
- Cualquier otra información relacionada a las necesidades del negocio.

10.1.2 Términos y condiciones de empleo.

- Clausulas o acuerdos de confidencialidad y no divulgación de la información.
- Cumplimiento de las leyes de protección de derechos de autor.
- Responsabilidad sobre la manipulación y almacenamiento de información.
- Cumplimiento de las disposiciones establecidas en la ley orgánica de prevención, condiciones y medio ambiente de trabajo.
- Aceptación de los términos y condiciones del código de conducta de la organización.

10.2 Durante el empleo.

10.2.1 Responsabilidades de la Dirección

Las responsabilidades de la dirección deberán incluir los siguientes lineamientos:

- Velar por el cumplimiento de la política de seguridad de la información y procedimientos establecimientos.
- Establecer planes de la concientización, capacitación y adiestramiento de los procedimientos de seguridad y el uso correcto de los medios para el procesamiento de la información, con la finalidad de minimizar los posibles riesgos de seguridad.
- Establecer medidas disciplinarias formales para el incumplimiento, desviación o riesgo de seguridad.

10.2.2 Toma de conciencia, educación y formación en la seguridad de la información.

- Todos los empleados de la organización, contratistas y usuarios de terceras partes deberán recibir entrenamiento apropiado de las políticas, procedimientos, responsabilidades legales y controles del negocio, así como de las buenas prácticas en el uso de los recursos.
- El entrenamiento deberá comenzar con una inducción formal del proceso designado para introducir la política de seguridad de la

organización y las expectativas, antes conocer acceso a la información o al servicio.

10.2.3 Proceso disciplinario.

- Deberá existir un proceso formal disciplinario para empleados que han cometido un a apertura en la seguridad.
- El proceso disciplinario no deberá comenzar sin una verificación previa de que la apertura de la seguridad ha ocurrido.
- El proceso disciplinario deberá asegurar un correcto y justo tratamiento a los empleados que son sospechosos de cometer apertura en la seguridad.
- Deberá proveer medidas graduales acordes con la naturaleza, la gravedad de la apertura y su impacto en el negocio. En casos serios de mala conducta, el proceso deberá permitir la desincorporación definitiva del agresor y eliminar sus privilegios de acceso.

10.3 Finalización o cambio de empleo.

- **Objetivo:** Asegurar que los empleados, contratista y usuarios de terceras partes salgan de la organización o cambian el empleo de una manera ordenada.

10.3.1 Responsabilidades de terminación

Authenticsing deberá ser garante del cumplimiento de los procedimientos de seguridad para desincorporar o realizar traslados internos de empleados, contratista y usuarios de terceras partes. Se deberá prestar atención a los siguientes aspectos:

- Ratificar el cumplimiento de los acuerdos de confidencialidad y no divulgación de información.
- Solicitar la devolución o movilización de equipos y herramientas de trabajo.
- Tramitar la revocación o actualización de controles y privilegios de accesos, tanto físicos como lógicos.
- Realizar el anuncio organizacional de los movimientos realizados.
- Todos los empleados, contratista y usuarios terceras partes deberán devolver los activos de la organización que están bajo su responsabilidad o que le fuera asignado durante su contratación.
- Establecer mecanismo y documentación de la migración y transferencia de data, conocimientos e información de los procesos críticos manejados por el personal a desincorporar o trasladar, es decir, transferencia del know how de los procesos que realizaba la persona.

11. GESTION DE ACTIVOS.

Destinado a mantener una adecuada política de protección de los activos que posee Authenticsing, estos activos deben ser identificados y clasificados con base al valor estratégico y/o crítico del mismo, de modo que en caso de inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos.

- Objetivos: Identificar y garantizar los activos de la organización y definir las responsabilidades de protección adecuadas.

11.1 Responsabilidad por los activos.

11.1.1 Inventario de activos.

En Authenticsing mantiene un adecuado inventario y control de sus activos, tanto físico (hardware) como lógico e intangible (Software) donde cada área es responsable de mantener actualizado el inventario de activos, esto quiere decir que Authenticsing identificará los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación. El Responsable de cada Unidad Organizativa involucrada deberá tener un inventario con dicha información y deberá actualizarlo ante cualquier modificación de la información registrada y revisarlo según lo especificado en el plan de seguridad.

. Algunos ejemplos de activos son:

- **Datos e Información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, manual y de operación de AUTHENTICSING.
- **Software y Programas:** software de aplicaciones, sistemas operativos, etc.
- **Hardware y Equipos**: equipamiento informático (procesadores, monitores, computadoras, portátiles, módems), equipos de comunicaciones (routers, fax, teléfonos, central telefónica), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, entre otros.
- **Proveedores y Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (iluminación, energía eléctrica, etc.).
- **Interfaces y Conexiones:** Todas los enlaces y conexiones presentes en la plataforma de certificación y en la oficina administrativa.

11.1.2 Propiedad de los activos

Toda la información y activo de inventario asociados a los recursos para el

tratamiento de la información deberán permanecer en las áreas designada por la Authenticsing.

11.1.3 Uso aceptable de los activos

Se deben identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

11.1.4 Devolución de los activos

Todos los empleados y usuarios de terceras partes deberán devolver todos los activos de la organización que estén en su posesión y/o responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.

También Controlar la copia no autorizada de información desde el periodo de aviso de finalización hasta que se materializa la devolución y borrado de datos.

11.2 Clasificación de la información.

- **Objetivo:** los activos de la información serán clasificados de acuerdo al valor estratégico y/o criticidad de la misma.

- **Estrictamente confidencial:** Todo activo de la información, relacionado con la dirección operacional y/o estratégica de la organización; documentos y/o materiales que requieran el más alto grado de protección, cuyo conocimiento y divulgación por parte de la personas no autorizadas causen graves daños a la organización, a este grupo corresponde:
  - Planes de contingencias, planes operacionales y de áreas estratégicas vitales para la continuidad operativa de la organización, así como la seguridad de las instalaciones de la organización.
  - Mapa de la arquitectura de la plataforma tecnológica de la organización.
  - Información crítica relacionada directamente con los procesos modulares de la organización y cuya divulgación la ponga en peligro.
  - Información correspondiente a la gestión de incidentes y diagnóstico de seguridad.
  - Las Claves de máxima privilegio de los sistemas y/o aplicaciones, así como toda documentación pertinente a la misma.
  - Información, data y registro de los clientes de la organización.
  - Cualquier otro activo de la información que permita conocer gran parte de las

operaciones de la organización.

- ❖ Manuales y documentación de operación, gerencia y comercial que solo compete a la organización.

- ➢ **Confidencial:** a los activos de información relacionados con el personal, clientes, información financiera, técnica, administrativa y cualquier información sensible de la organización, cuyo conocimiento y divulgación a personas no autorizada, causen daños a la organización; tendrán esta clasificación los siguientes activo de la información:
  - ❖ Contraseñas y/o claves de accesos a los sistemas y aplicaciones de la plataforma tecnológica de la organización.
  - ❖ Toda información correspondiente a sistemas y aplicaciones de la plataforma tecnológica de la organización.
  - ❖ Expedientes y registros de transacciones operacionales a administrativos entre la organización y terceros.
  - ❖ Informe de auditoría interna y externa.
  - ❖ Informe de eventos de seguridad física y lógica.
  - ❖ Proyectos tecnológicos y de infraestructura
  - ❖ Cualquier otro activo de información que el comité o jefe del departamento así lo establezca.

- ➢ **De uso interno:** todo activo de información que requiera medidas de protección no especiales, cuyo acceso y manipulación deba ser realizado anteponiendo los intereses de la organización; estos activos que tendrán esta clasificación son:
  - ❖ Programas de entrenamiento
  - ❖ Políticas de seguridad de la información.
  - ❖ Normas internas.
  - ❖ Procedimientos generales.
  - ❖ Lineamientos internos.
  - ❖ Informes de gestión, una vez publicadas por el ente competente.
  - ❖ Toda aquella información que no sea clasificada como “Estrictamente confidencial” o “Confidencial”

- ➢ **De uso público:** Es toda aquello activos de información que no requieran se ninguna medida de protección y que no cumpla con los criterios de clasificación Estrictamente confidencial, Confidencial o de uso interno.

11.3 **Manejos de los soportes.**

- ➢ **Objetivo:** proteges la información en el nivel de soportes en los que se

encuentra ya sea en papel o soporte electrónicos.

- **Gestión de medios extraíbles:** la gestión de medios o soporte removibles en los que se almacenen información y data de la organización puede suponer una brecha importante en la seguridad de la información por lo que la norma propone mantener un control específico para este tipo de soportes o dispositivos removibles, para gestionar los soportes extraíbles se debe considerar:

  - Minimizar la necesidad de usos de los dispositivos extraíbles o removibles.
  - Mantener un registro de los dispositivos extraíbles para limitar la posibilidad de pérdida de datos y uso autorizado por la organización.
  - Mantener un seguimiento a la transferencia de información de los medios removibles mediante herramientas tecnológicas que permita realizar la trazabilidad de la información transmitida a estos medios.
  - La junta directiva, el Gerente general, los directores y jefes de oficina, deben controlar el ingreso y salida de los equipos de cómputo y medios extraíbles de almacenamiento de información de las instalaciones de la organización.
  - Los soporte extraíbles o medios removibles no deben ser utilizados en sitios públicos como un café internet, así mismo, debe tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.
  - Renovar dispositivos con un periodo determinado para evitar la degradación de datos necesarios e importantes.
  - Proteger la información almacenada con copias de seguridad en soportes independientes.
  - Encriptar datos para proteger aquellos que se consideren importantes.
  - Documentar los procedimientos de autorización.

- **Eliminación de soportes:** Establecer procedimientos para la eliminación segura de soportes a la finalización de su uso, tratar de minimizar o evitar que los datos sensibles o confidenciales puedan ser recuperados una vez que el dispositivo se da de baja mediante procedimientos de eliminación segura. Se deben disponer los siguientes criterios:
  - Establecer un proceso de eliminación segura de datos que no permita su recuperación.
  - Identificar que dispositivos requieren de un proceso de eliminación segura.
  - Mantener un registro dispositivos que han sido dados de baja de forma segura por contener información sensible.
  - Los soportes o medios removibles que contienen información confidencial se deben disponer en forma segura, mediante destrucción o el borrado de datos antes de ser reutilizados o dados de baja.

- ❖ La información en las cintas de backups que contienen información pública clasificada o información pública reservada se debe cifrar, además deben estar protegidas en un lugar seguro y bajo llave, el lugar que disponga

- ➢ **Transferencia de soportes o medios físicos:** Se trata de establecer un control para proteger la información cuando los soportes necesitan ser trasladados entre distintas ubicaciones. Para ello deberemos establecer un control sobre:
  - ❖ Para la transferencia de medios físicos (Información en carpetas selladas, computadores, dispositivos móviles, tablets, etc.) se debe seguir las directrices del Procedimiento de Gestión de Activos y sus documentos relacionados (mensajería externa o interna - tabla controles según clasificación de información).
  - ❖ Se debe llevar un registro que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.
  - ❖ Llevar un registro de salida de los soportes para su cotejamiento y mantener una lista de la misma.

12. CONTROL DE ACCESOS.

12.1 Requisitos de negocio para el control de acceso

- ➢ **Objetivo:** Establecer requisitos mínimos que están orientadas para controlar y monitorizar el acceso a los medios de información de Authenticsing por medio de sus redes, sistemas y aplicaciones, de acuerdos a las políticas definidas por Authenticsing.

12.1.1 Política de control de los accesos:

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información Authenticsing implementa procedimientos formales para controlar la asignación de acceso a los sistemas de información, bases de datos y servicios de información, tanto de y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

El principio básico para la elaboración de estas reglas es:

- ➢ La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información
- ➢ La concesión de esos privilegios solamente son por el tiempo que sea

necesario para el desarrollo de las tareas

- El principio básico para la elaboración de estas reglas es:
  - La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información
  - La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas

12.1.2 Acceso a las redes y a los servicios de red.

Se debe establecer un control de acceso a la red, tanto interna como externamente, implantando medidas de seguridad y procedimientos de autorización de acceso.

- Se debe establecer autenticación de usuarios en los accesos remotos a través de técnicas criptográficas, servicios de VPN, líneas dedicadas privadas, verificación de origen de conexión, etc.
- Se protegerán los servicios de red, puertos de configuración y diagnóstico remoto. Cuando no sean necesarios estarán deshabilitados.
- La red debe estar segmentada según su criticidad.
- Se debe contar con controles de conexión a la red (filtros, reglas, etc.), de enrutamiento y de identificación del equipamiento en la red.
- Políticas y normas de seguridad para el acceso del servicio de correo corporativo.

12.1.2.1 Redes wifi.

- El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.
- Los dispositivos móvil, laptops son registrados sus dirección MAC para tener acceso a la reb wifi.
- El acceso a la red Wi-Fi de Authenticsing para los visitantes debe realizarse por la red destinada para estos accesos a visitantes, de no conocer este acceso se debe solicitar al coordinador de tecnología Ayuda para su debida activación.

12.1.2.2 Correo electrónico.

El correo electrónico institucional de Authenticsing le permite al usuario utilizar su buzón de mensaje a través de la red interna de Authenticsing. El Coordinador de tecnología será quien designe la aprobación para asignar una clave donde el usuario podrá acceder a su buzón, enviando y recibiendo mensajes solo a usuarios definidos en la red. Correo

electrónico externo (Internet): le permite al usuario enviar y recibir mensajes a través de Internet, una vez autorizado por el coordinador de tecnología, usando la misma clave del correo electrónico interno. Esta modalidad será disponible para aquellos usuarios cuyas responsabilidades del puesto este prevista las comunicaciones con organizaciones o personas externas (clientes, proveedores, etc.). El uso de correo interno y externo se encuentra restringido para actividades de la empresa, todo correo personal deberá ser envidos a través de la compañía de servicios de correo electrónico con la cual mantenga registro cada trabajador.

- Relativas al uso: El servicio de correo electrónico en todas sus modalidades debe ser utilizado únicamente para las comunicaciones relacionadas con las operaciones de la empresa, ningún usuario deberá utilizar este servicio con fines personales. El servicio del correo electrónico en cualquiera de sus modalidades no deberá usarse con fines comerciales, de publicidad o promoción de productos o servicios que no sean los establecidos por la empresa. El servicio del correo electrónico en cualquiera de sus modalidades no debe utilizarse para enviar “cadenas”, “pornografía”, “spamming” o cualquier otro que atente con las normativas de la empresa.

  La opción “contactos” del correo electrónico debe ser utilizada con fines netamente laborales, tales como: clientes, proveedores, etc.

  La agenda de reuniones, tanto interna como externa, las invitaciones a las mismas y el control de asistencia, deben ser controladas y registradas a través de la opción “calendario” provista en el correo electrónico, con el fin de centralizar y facilitar la coordinación y sincronización del tiempo de los participantes

12.1.2.3 Centro de Datos.

- **Controles de acceso físico:** Las áreas sensibles y críticas se resguardarán mediante el empleo de controles de acceso físico, los que serán definidos por el responsable de seguridad informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:
  - Supervisar o vigilar (cámaras de seguridad) a los visitantes de áreas donde estarán ubicados los servidores de la plataforma de certificación.
  - Registrar la fecha y horario de su ingreso y Registrar la fecha y horario de su ingreso y egreso

- ❖ Revisar y actualizar cada vez que exista un cambio los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Gerente General
- ❖ Revisar y auditar según lo contemplado en el plan de seguridad y riesgos, la efectiva ejecución de los controles de acceso a las áreas protegidas. Esta tarea la realizará la unidad de auditoría interna o en su defecto quien sea propuesto por el comité de seguridad y riesgos

➢ Seguridad perimetral: En la plataforma de certificación estará instalado un equipo de seguridad que permite controlar y proteger todo el tráfico y contenido de entrada y salida entre todos los puntos de conexión o el perímetro de la red a través de la siguiente configuración:

- ❖ ZONA 1: ZONA PÚBLICA. Equipos de la ZONA 1: Servidores que necesitan ser accedidos desde internet, y los servidores que necesitan tener acceso a internet. ZONA 2: ZONA PRIVADA. Equipos de la ZONA 2: Servidores Privados de la plataforma de certificación.

  Entre internet y la ZONA 1, solo se permitirán las conexiones mínimas necesarias para el acceso a los servicios de certificación que ofrece Authenolgy. Entre la ZONA 1 y LA ZONA 2 solo se permitirán las conexiones mínimas necesarias para la operación de la plataforma de certificación. Adicional, a las funcionalidades de firewall, el equipo de seguridad instalado tendrá habilitado las siguientes funciones: IDS/IPS y Antivirus.

12.1.2.4 Acceso por conexión remota.

Se define como acceso remoto cualquier conexión establecida desde fuera de la Entidad que requiere acceso a la red o aplicaciones internas de la ANM por parte de funcionarios, proveedores entre otros.

Para dichos accesos se debe tener en cuenta las siguientes consideraciones:

- ➢ Las conexiones remotas a los recursos de la plataforma tecnológica; deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas
- ➢ La autenticación para los accesos remotos debe complementarse con doble factor de autenticación y/o a través de la plataforma de seguridad.
- ➢ El trabajo remoto por VPN lo debe autorizar el coordinador de tecnología, conforme al procedimiento definido de solicitud de requerimientos, se valida la pertinencia de dicha solicitud y otorga el

privilegio, evaluando y aplicando las medidas de protección adecuadas que garanticen una conexión segura.

- El acceso remoto a los servidores debe estar controlado por las políticas y normas de seguridad de la información que implemente Authencsing para el ingreso por este servicio, es decir quién puede o no ingresar por este servicio, teniendo presente que este servicio debe ser autorizado únicamente para los administradores de los servidores, los usuarios o proveedores fuera de la oficina no deben tener estos accesos o llamado a este servicio.

- **Trabajo Remoto por VPN:** El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la oficina administrativa. El trabajo remoto sólo será autorizado por la alta dirección, conjuntamente con el Gerente General y el Coordinador de Tecnología, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes. Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia. Para ello, se establecerán en el plan de seguridad normas y procedimientos para el trabajo remoto. Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos

Para sus servicios externos de Authenticsing, sus aplicaciones deben forzar y utilizar autentificación mediante protocolo HTTPS.

12.2 Gestión del Acceso de usuarios

- Objetivo: Asegurar el acceso del usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.

12.2.1 Acceso a los usuarios.

Los procedimientos definidos por Authenticsing para administrar los privilegios de acceso de los usuarios a la información de Authenticsing deben comprender la asignación, la modificación y la revocación de los permisos. Todos los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y deben de tener en cuenta por lo menos:

- Utilizar un identificador único para cada usuario, de esta forma puede

vincularse a los usuarios y responsabilizarles de sus acciones.

- Comprobar la autorización del usuario por el propietario del servicio.
- Verificar la adecuada del nivel de acceso asignado al propósito del negocio y su consistencia con la política de seguridad.
- Entregar al usuario una relación por escrita de sus privilegios, derechos y condiciones de acceso, solicitando su firma en señal de conformidad.
- Mantener registros de documentos de todos los autorizados para usar el servicio.
- Revocar inmediatamente las autorizaciones de acceso a los usuarios que han dejado o cesado con Authenticsing.
- Revisar periódicamente los identificadores y cuentas de usuarios, con la finalidad de eliminar registros redundantes.
- El coordinador de tecnología, asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada grupo y/o proceso.
- El acceso de un usuario debe ser limitado sólo a la información requerida para el desarrollo de sus funciones.

12.2.2 Gestión de privilegiados.

- Asignación de privilegios a los empleados según los principios de necesidades de uso y caso por caso y en concordancia con la política de control de acceso.
- Mantener un proceso de autorización y registro de todos los privilegios asignados. No se otorgaran privilegios hasta que el proceso de autorización haya concluido.
- Promover el desarrollo y uso de programas que no permitan la asignación de privilegios.
- Los accesos a la información o sistemas de información no deben otorgarse por los administradores de Base de Datos y de Aplicaciones del servicio hasta que se hayan completado los procedimientos de autorización.

12.2.3 Remoción o ajuste de los derechos de acceso.

El acceso a los sistemas debe ser suspendido para todo funcionario o colaborador de Authenticsing que se encuentre en licencia, permisos, vacaciones, entre otras novedades; si por necesidad del negocio se requiere mantener habilitado, únicamente para cargos de alto nivel, para los demás cargos si existen funciones que se deban reasignar para dar continuidad durante dichas novedades, los jefes o delegados deben realizar las solicitudes de acceso necesarias a los colaboradores que ejecutaran las

actividades, una vez cumplido el plazo se debe solicitar retiro de los permisos.

13. CONTROLES CRIPTOGRÁFICOS.

- Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de procesamiento de información y la información de la organización.

13.1 Políticas sobre el empleo de controles criptográficos.

Los controles criptográficos están enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, como política de seguridad Authenticsing se impone establecer normar de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad.

Para el caso de la plataforma tecnológica de Authenticsing implementado en sus sistemas de certificados electrónicos, Los controles criptográficos se utilizan como un control añadido que proporciona confidencialidad, autenticidad, no repudio y autenticación.

- Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.
- Los administradores de bases de datos de de Authenticsing deben establecer una estrategia para cifrar las bases de datos críticas de Authenticsing, velando por no afectar el desempeño del sistema de información.
- Realizar la entrega de los certificados digitales generados con el debido procedimiento para su aplicación y uso.
- Realizar las configuraciones requeridas para el uso y administración de los certificados de firma digital.
- Prestar soporte técnico para la configuración de los usuarios y soluciones adoptadas para controles criptográficos.
- Realizar revisiones periódicas a las herramientas de uso criptográfico (Tokens, Firma Digital, etc.), con el fin de detectar fallas o vulnerabilidades.
- Identificar los puertos USB para quienes estén autorizados para la firma digital y contar con este inventario con el fin de dar seguimiento al buen uso de la información.

13.2 Gestión de claves.

En Authenticsing la gestión de contraseñas establece las reglas que las contraseñas de un servicio deben cumplir, como la longitud y el tipo de caracteres

permitidos y no permitidos. Además, la política de contraseñas puede especificar que no se permita la entrada de un término que aparezca en un diccionario de términos prohibidos.

Para las contraseñas, puede especificar los estándares siguientes y otras reglas:

- Longitud mínima y máxima
- Restricciones de caracteres
- Frecuencia de reutilización de contraseñas
- Nombres de usuario o ID de usuario prohibidos
- Especifique una duración mínima de la contraseña

13.2.1 Relativas a la construcción de las contraseñas.

Se recomienda la construcción de contraseñas que sean fácilmente recordables y además cumplan con las siguientes normativas:

- Además de las letras (A - Z), incluya dígitos (0-9), caracteres de puntuación y símbolos matemáticos (&%#)?=+*/).
- Usar como mínimo ocho caracteres de largo.
- No utilice ningún lenguaje jerga, dialecto, etc.
- No se base en información personal tales como: fecha de nacimientos, nombre personal o familiares, teléfonos, cedula de identidad, entre otros.
- No repita las últimas contraseñas utilizadas.

Trate de crear contraseñas que cumplan con lo expuesto.

14. SEGURIDAD FÍSICA Y DEL AMBIENTE.

14.1 Áreas seguras

- Objetivos: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización.

14.1.1 Perímetro de seguridad física.

14.1.1.1 Acceso a sus oficinas administrativas.

Authenticsing en sus instalaciones administrativa tiene implementado un sistema de control de acceso físico mediante huella digital, aparte que solo el personal autorizado y que labora para Authenticsing tiene acceso a sus oficinas.

Además cuenta con sistema de seguridad de circuito cerrado (CCTV), para otorgar la mayor seguridad posible tanto a sus empleados como a los clientes de Authenticsing.

14.1.1.2 Data center.

Autenticsing cuenta con los servicios de alojamientos de sus servicios en DaycoHost cuyas instalaciones cuenta con las políticas y medidas seguridad en la que se puede detallar que cuentan con un sistema de control de acceso por huella biométrica por cada piso y a sus diferentes áreas de data center. Adicionalmente, cada piso cuenta con una recepción donde se controla el ingreso y salida de terceros, y el ingreso y salida de elementos, tanto de funcionarios como de terceros. A sí mismo DaycoHost exige a sus clientes y proveedores que gestionen o procesen información de acceso a las instalaciones de su data center, cumplir con las políticas de seguridad de DaycoHost y las que disponga el proveedor en sus instalaciones..

El Data center cuenta con mecanismos que cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga, igualmente debe contar con sistemas mecánicos para control de incendios, impedir el acceso a personal no autorizado, consumo de alimentos, bebidas o cigarrillo.

Para el caso de DaycoHost que es el proveedor de servicio de alojamiento, establece criterios de seguridad:

- Medidas de control de presencia y controles de acceso
- Medidas de protección volumétrica como detectores de presencia o de humo / fuego
- Medidas de control de actividad
- Cámaras de seguridad
- Políticas de uso de las instalaciones
- Medidas de control de información
- Medidas de control de áreas de carga, Se debe tener en cuenta que las áreas de carga nunca deben tener acceso directo a áreas seguras.

14.2 Equipamiento

14.2.1 Ubicación y protección del equipamiento.

14.2.1.1 Data Center.

Controles que cuenta DaycoHost para proteger los equipos de daños

ambientales y accesos no autorizados

- El Datacenter está ubicado de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por la Oficina de Tecnología e Información y seguridad.
- Se hace seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar adversamente el Datacenter.
- Evitar accesos no necesarios
- Proteger los equipos de áreas sensibles como centros de datos o salas de servidores
- Controles de protección en lugares de almacenamiento de equipos si estos contienen información
- Medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.)
- Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos
- Medidas de protección contra radiaciones
- Deben establecerse pautas para comer, beber y fumar cerca del equipo para evitar daños o simplemente evitar que los empleados estén en contacto con los equipos si no están trabajando en ellos.
- Registrar la fecha y horario de su ingreso y Registrar la fecha y horario de su ingreso y egreso
- Revisar y actualizar cada vez que exista un cambio los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Gerente General
- Revisar y auditar según lo contemplado en el plan de seguridad y riesgos, la efectiva ejecución de los controles de acceso a las áreas protegidas. Esta tarea la realizará la unidad de auditoría interna o en su defecto quien sea propuesto por el comité de seguridad y riesgos

14.2.2 Seguridad del Cableado.

14.2.2.1 Data Center

El Datacenter cumple con la normatividad de cableado estructurado y está debidamente certificado. A sí mismo DaycoHots exiges a sus clientes y proveedores de servicios informáticos, cumplir con las políticas de seguridad de Authenticsing.

14.2.2.2 Oficinas administrativas.

Authenticsing cumplen con las normatividad de cableado estructurado en su sede administrativas utilizando material certificado.

14.2.3 Mantenimiento de Equipos.

Authenticsing establece como política ejecutar planes anuales de mantenimiento de la infraestructura tecnológica de Authenticsing, esto aplica para sus equipos en la sede administrativas y los equipos alojados en el Data Center de Daycohost.

14.2.4 Seguridad en la reutilización o eliminación de equipos

Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información de Authenticsing que allí se encuentre almacenada (en caso de ser necesario).Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma. Ver indicaciones adicionales en el procedimiento de borrado seguro.

14.2.5 Política de escritorio limpio.

Todos los empleados de Authenticsing deben conservar su escritorio libre de información propiedad de Auhenticsing, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

- Los computadores deben cargar por defecto el fondo de pantalla de Authenticsng, éste no debe ser modificado y debe permanecer activo
- Los usuarios son responsables y asumen las consecuencias por la pérdida de información que este bajo su custodia. Se prohíbe el almacenamiento de información personal en los computadores de Authenticsing. Elescritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

15. SEGURIDAD DE LAS OPERACIONES.

- Objetivo: Asegurar la correcta operación en las instalaciones de procesamiento de información

15.1 Documentación de Procedimientos Operativos.

Authenticsing cuenta con procedimientos documentados de trabajo debidamente documentados para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

- Los procedimientos de operación deben documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
- La formalización y el establecimiento de un procedimiento que permita el adecuado control de los cambios en los sistemas e instalaciones de procesamiento de información.
- Supervisar y adaptar el uso de recursos, así como formular proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido de los sistemas.
- La separación de los recursos para desarrollo, prueba y producción, con el propósito de reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.
- La segregación de las tareas y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la institución.

15.2 Respaldo de la información.

El Gerente General y el Consultor de Tecnología determinarán los requerimientos de respaldo de cada software y dato en función de su criticidad. Con base a ello, se definirá y documentará un esquema de respaldo de la información. Existirán respaldos diarios, semanales, mensuales y anuales. Los operadores de informática controlarán la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de la empresa. Los sistemas de respaldo deberán probarse periódicamente.

La clave privada del Authenticsing requerirá tener un cuidado especial en cuanto a su respaldo, en la plataforma de certificación debe estar almacenada en un hardware de seguridad, y el respaldo almacenado, para la recuperación en caso de desastre, debe ser accedido solamente por la alta dirección. Se definirán procedimientos para el respaldo de la información, que deberán considerar los siguientes puntos:

- Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Almacenar en una ubicación remota copias recientes de información de respaldo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como

para evitar daños provenientes de un desastre en el sitio principal.

- Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de respaldo.
- Probar periódicamente los medios de respaldo.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos. Adicionalmente, todos los respaldos ejecutados en la plataforma de certificación y en la oficina administrativa deben ser almacenados en una bóveda ubicada en un lugar alterno al centro de datos y a la oficina administrativa. El acceso a la información almacenada en la bóveda debe estar limitado exclusivamente al personal que labora en el AUTHENTICSING, según si nivel de criticidad y confidencialidad

15.3 Protección ante software malicioso.

15.3.1 Controles ante software malicioso

El consultor de Tecnología definirá controles de detección y prevención para la protección contra software malicioso y adicionalmente implementará dichos controles. El consultor de tecnología desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

- Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de Authenticsing contra códigos maliciosos
- El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.
- El único servicio de antivirus autorizado en Authenticsing es el asignado directamente por la coordinación de tecnologia, el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura
- El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.
- El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.
- Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por la

coordinación de tecnologia.

15.3.1.1 Relativa al uso.

- Todos los computadores deben contar con la instalación del software contra software malicioso previamente aprobado por la empresa, debidamente instalado, configurado y activo en la memoria de cada desktop, laptop y servidor tanto de la sede administrativa de como del centro de datos de Authenticsing.
- Todos los computadores deben contar con la instalación de la última versión actualizada del software contra software malicioso.
- El software contra el software malicioso, así como la lista de definiciones de software malicioso se debe mantener actualizados diariamente y de forma automática.
- El software contra software malicioso está configurado para revisar semanalmente y de forma automática todos los equipos (laptops, desktops y servidores) de la sede administrativa de Authenticsing.
- Las actualizaciones críticas de seguridad deben instalarse de forma automática e inmediatamente luego de la publicación por parte del proveedor del software de protección contra software malicioso. Los operadores de informática serán responsables de verificar que las actualizaciones del software de protección contra software malicioso se hayan realizado y cumplido de forma efectiva.

15.3.1.2 Relativa al software antivirus instalado.

Todos los computadores deben tener la última versión disponible del software e protección contra software malicioso, por lo cual se deberá realizar una revisión mensual y anual con el proveedor del mismo para realizar la debida actualización si es necesario.

15.3.1.3 Relativas a la prevención contra software malicioso.

No permitir abrir archivos, macros anexos, correos de remitentes desconocidos, sospechosos, o fuentes poco confiables. De acuerdo al punto anterior, borre inmediatamente todo archivo de remitentes sospechosos, vacié su papelera o comuníquese directamente con el área de Informática quien le dará la asesoría respectiva. Está prohibido pasar cadenas, publicidad o cualquier otro archivo de igual procedencia, en concordancia con la política del uso aceptable del correo electrónico. Ningún usuario debe bajar archivos de lugares desconocidos o sospechosos. En caso de que requiera algún material en particular para el desempeño de sus funciones contacte al Consultor de Tecnología

para su respectiva asesoría. Ningún usuario debe ejecutar aplicaciones si el software de protección contra software malicioso está inactivo (Deshabilitado).

15.3.1.4 Relativa a la conducta en caso de un contagio de por software malicioso.

En caso de un contagio de por software malicioso, sospecha de infección o conducta inapropiada de un programa o del equipo, el usuario deberá apagar el computador e informar inmediatamente al área de Informática.

15.4 Respaldo de la información.

En Authenticsing de debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la coordinación de tecnología de la Información define el Procedimiento de Copias de Respaldo e Instructivo, que definen las actividades para la estrategia de backup requeridas; además:

- La coordinación de tecnología debe establecer las políticas de copias de seguridad desde la herramienta de backup, para los sistemas de información y bases de datos.
- Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la Oficina de Tecnología e Información.
- Todas las copias de respaldo deben ser almacenadas en un área adecuada y con control de acceso, y aplicar los controles para la protección de los medios de respaldo.
- . Todas las copias de respaldo deben contemplar un plan de continuidad del negocio, orientado a evitar la pérdida de la información al contemplar un sitio secundario para su preservación.
- Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.
- Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la Entidad, motivo por el cual no debe ser divulgada a terceros, salvo autorización expresa de Authenticsing.

15.4.1 Verifique su validez

Authenticsing comprueba que las copias son válidas, mediante el proceso de verificación de la validez de las copias de seguridad

mediante algún proceso de restauración simulado o en algún equipo de prueba.

15.4.2 Medios de recuperación

Los medios de recuperación son tan importantes como las propias copias de seguridad por lo que deberemos tener en cuenta el mantenimiento en perfecto estado de funcionamiento de los medios que nos permitirán la restauración de las copias cuando las necesitemos

15.4.3 Mantener registros

Authenticsing mantendrán unos registros de las copias de seguridad como parte de un cronograma o plan de mantenimiento de copias de seguridad. Así como también se mantendrán un registro de las pruebas de validez de dichas copias.

16. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

16.1 Gestión de la continuidad del negocio.

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles de la empresa. El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la empresa puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Planificar e implementar la Continuidad de Negocio en Authenticsing, debe ser un aspecto fundamental teniendo en cuenta no sólo los recursos tecnológicos, sino también activos de información crítica de los procesos, los cuales han sido definidos y estructurada.

Para esto Authenticsing contempla en sus planes de contingencia lo siguientes:

- Se deben realizar pruebas periódicas a los controles de Continuidad de Negocio y de continuidad de la Seguridad de la Información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
- Los responsables de los procesos e información deben asegurar que se

actualicen los Planes de Continuidad de Negocio posterior a los cambios en la infraestructura tecnológica con respaldo de la coordinación de tecnología.

- Contemplar un sitio alterno, donde los controles implementados en el ambiente de producción deben ser consistentes con el sitio alterno.
- Los cambios de seguridad en el ambiente de producción deben ser aplicados de la misma forma para el ambiente de contingencia.
- El Plan de Continuidad de Negocio debe ser protegido contra accesos no autorizados, contemplando a su vez copias de respaldo y que éstas sean resguardas en un sitio externo con la protección adecuada tanto física como medioambiental.

16.1.1 Administración de la continuidad de la empresa.

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de negocio Authenticsing. Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la empresa frente a interrupciones imprevistas.

16.1.2 Implementación de la continuidad de la seguridad de la información.

16.1.2.1 Estructura de gestión y responsables.

La responsabilidad en la continuidad y recuperación de esta actividad será llevada a cabo por la alta dirección y el Consultor de Tecnología, y según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la empresa.

16.1.2.2 Funciones.

- Gestionar los incidentes de seguridad de la información
- Mantener los niveles de seguridad de la información ante emergencias
- Recuperar los sistemas de información

16.1.2.3 Documentación y procedimientos.

Los procesos de cómo se va gestionar un evento destructivo o el plan de continuidad de negocio, está documentado el documento “DPL-001 - Plan de Continuidad de Negocio.”

16.2 Redundancias.

- Authenticsing debe establecer e implementar un Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

- Authenticsing debe realizar pruebas periódicas al DRP, con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

17. CUMPLIMIENTO.

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

- Constitución de la República Bolivariana de Venezuela. Artículo 60
- Ley Especial Contra los Delitos Informáticos, Título II, Capítulo I, De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información.
- Ley de Infogobierno.
- Ley sobre mensajes de datos y firmas electronicas.

18. REVISIÓN, APROBACIÓN Y MODIFICACIÓN.

Las funciones y responsabilidades de los distintos niveles de AUTHENTICSING, respecto al manejo, control y resguardo del presente documento, se encuentran definidos en el Documento de la Política para el Establecimiento de Funciones y Responsabilidades.

19. MARCO LEGAL, NORMATIVO Y DOCUMENTACIÓN APLICABLE.

- Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento.
- Normativa de SUSCERTE.
- Normativa AUTHENTICSING.
- Norma ISO 9000:2015.
- Norma ISO/TR 10013:2001.
- Estándar Internacional ISO/IEC 17779.
- Estándar internacional ISO/IEC 27001:2013.
- Estándar Internacional COBIT 4.0.

20. FUNCIONES Y RESPONSABILIDADES.

Los procesos asociados a la revisión, aprobación, modificación o ajuste de la

documentación del PSC AUTHENOLGY, serán regulados por el “Documento de la Política de Documentación y Gestión Documental”.

--- Fin de Documento ---