AUTHENOLOGY
FIRMA ELECTRÓNICA

AUTHENTICSING C.A.

Plan de Seguridad de la Información.

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 19:49:53 -04'00'

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Plan de la Seguridad de la Información.		
Tipo de Documento	Documentación Técnica sobre Planes de Seguridad.		
ID	DPL-002		
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**	**- 48 -**
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.

Plan de la Seguridad de la Información.

3. CÓDIGO DEL DOCUMENTO

DPL-002

4. INTRODUCCIÓN.

El presente documento constituye el Plan de la Seguridad de la Información parte de los Proveedores de Certificados **AUTHENTICSING** a fines de comunicar, informar y documentar cada uno de los procesos de certificación, para ofrecer una mejor y sencilla comprensión e entendimiento por parte de la Alta dirección, Clientes, Proveedores, Personal y otros interesados de AUTHENTICSING**.**

El Plan de la Seguridad de la Información, permite a la Alta dirección, Clientes, Proveedores, Personal, y otros interesados del PSC, dar a entender cada uno de los desarrollos y subdesarrollos involucrados en las etapas de vida de los certificados electrónicos; documentar los procesos de recuperación ante accidentes, uso de claves criptográficas y proporcionar una perspectiva general de los equipos e infraestructura que sostiene el esquema de seguridad de AUTHENTICSING**.**

Las políticas de los certificados autorizan a la Alta dirección, Clientes, Proveedores, Personal, y otros interesados de AUTHENOLOGY, comprender y conocer el uso autorizado(legal) de cada uno de los tipos de certificados que emite DE AUTHENTICSING , su configuración, organización, estructura y sus funciones emitidas por los certificados. La Alta dirección, Clientes, Proveedores, Personal y

otros interesados de AUTHENTICSING que usen los certificados electrónicos emitidos por AUTHENTICSING**,** tendrán un compromiso de ofrecer o entregar cumplimiento al actual documento Plan de la Seguridad de la Información, serán conscientes y responsables por las consecuencias procedentes del manejo y práctica no ajustado de un certificado electrónico o de la infracción de las instrucciones contenidas en el actual documento.

5. TÉRMINOS Y DEFINICIONES.

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

- **Continuidad del negocio:** Es la "capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades operativas y comerciales en un nivel aceptable previamente definido"
- **Recuperación ante desastres:** se refiere "al proceso, políticas y procedimientos relacionados con preparar la recuperación o continuación de la infraestructura tecnológica crítica de una organización después de un desastre natural o producido por el hombre".

- **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 de 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 DE 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 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 de 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.
  - 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:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de authenticsing que así lo requieran.
- **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).

6. OBJETIVO.

El presente documento es de presentar e informar el Plan de Seguridad de la Información, el cual es coherente con las Políticas de Seguridad que posee el PSC AUTHENTICSIN, que permite mostrar un nivel de confianza consistente con los objetivos del negocio.

7. ALCANCE.

En referencia al Plan de Seguridad de la Información tiene como propósito describir los requerimientos de seguridad de la información y los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debe delinear las responsabilidades y conductas esperadas de los individuos que acceden a los sistemas. Por lo tanto, el Plan de Seguridad de la información describe las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC AUTHENTICSING.

8. POLÍTICA.

El alcance de AUTHENTICSING, tiene como finalidad de presentar las normas del proceso automatizado de verificación de identidad y gestión de certificados de firma y

certificados electrónicos de seguridad en cumplimiento del marco legal y las normativas dadas por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

9. LIMITACIONES.

Para el PSC AUTHENTICSING presenta las limitaciones, por lo complejo y la envergadura del proyecto, contara con los servicios de un aliado comercial el cual presenta la infraestructura tecnología adecuada para la implementación del PSC de AUTHENTICSING. El cual cumple con las normas de seguridad y las políticas de seguridad de la información; adecuándose a las normas que nos exige SUSCERTE para la implementación de un PSC.

10. DESCRIPCION.

EL plan de seguridad describe las acciones, operaciones, procedimientos y mecanismo que van de la mano con los objetivos de las políticas de seguridad del PSC AUTHENTICSING, el cual se considera implementar y evaluar con base a algunos controles de la ISO 27002:2013.

10.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La organización de la seguridad de la información es un proceso crítico y vital para el PSC AUTHENCSING, ya que la información es uno de los activos más valiosos que posee. A continuación, se presenta un plan general para el control la organización de la seguridad de la información:

10.1.1 Identificación de la información crítica.

Se debe identificar la información crítica que posee el PSC AUTHENCSING y establecer un inventario de los datos que se manejan en la organización.

10.1.2 Evaluación de riesgos.

Se debe realizar una evaluación de riesgos de la información crítica, para determinar los posibles peligros que enfrenta la información y establecer medidas para mitigarlos.

10.1.3 Implementación de controles de seguridad.

Una vez identificadas las amenazas, se deben implementar controles de

seguridad apropiados para proteger la información crítica. Esto puede incluir la implementación de firewalls, antivirus, sistemas de autenticación y autorización, y políticas de acceso a la información.

10.1.4 Educación y concienciación de los empleados.

Es importante educar a los empleados de PSC AUTHENCSING sobre la importancia de la seguridad de la información y cómo pueden contribuir a mantenerla segura. Esto puede incluir la realización de capacitaciones, el establecimiento de políticas claras y la realización de simulaciones de ataques y pruebas de penetración.

10.1.5 Monitoreo y evaluación continúa.

La seguridad de la información es un proceso continuo, por lo que es importante monitorear y evaluar regularmente los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.1.6 Plan de respuesta a incidentes.

Se debe establecer un plan de respuesta a incidentes para manejar el impacto de cualquier violación a la seguridad de la información que pueda ocurrir. El plan debe incluir un equipo de respuesta a incidentes, procedimientos de notificación y comunicación, y una estrategia de recuperación de datos.

10.1.7 Revisión y mejora continúa.

La seguridad de la información debe ser un proceso en constante evolución y mejora. Se deben realizar revisiones periódicas de los controles de seguridad y el plan de respuesta a incidentes para identificar áreas de mejora y hacer ajustes necesarios.

10.1.8 Organización interna

10.1.8.1 Funciones y responsabilidades de la seguridad de la información.

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

10.1.8.2 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.

10.1.9 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.

- Para este el gerente general se pondrá en contacto con las autoridades de SUSCERTE en caso de que la plataforma tecnológica del PSC AUTHENTICSING se hubiese visto comprometida por alguna de causa de fuerza mayor y aplicar los procedimientos del Plan de continuidad del negocio y recuperación ante desastres.

En caso de que se sospeche de violación de un hecho delictivo (Hurto,

robo, tráfico de información entre otros).

- Para este caso el gerente general del PSC AUTHENTICSING se pondrá en contacto con las autoridades del CICPC, específicamente con la división de delitos informáticos, según sea el caso del hecho.

10.1.10 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.

10.2 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

La seguridad ligada a los recursos humanos es un aspecto crítico de la seguridad de la información, ya que los empleados pueden ser una fuente de vulnerabilidades y riesgos. A continuación, se presenta un plan general para la seguridad ligada a los recursos humanos:

10.2.1 Políticas y procedimientos claros.

Es importante establecer políticas y procedimientos claros para el manejo de la información y los sistemas de la organización. Esto debe incluir la definición de roles y responsabilidades, la clasificación de la información, las políticas de acceso y uso, y la gestión de contraseñas.

En Authenticsing se procederá a realizar los procedimientos y manuales para el manejo de la información, esto con la finalidad de manera correcta las actividades y funciones en el PSC AUTHENTICSING.

10.2.2 Verificación de antecedentes.

Se debe realizar una verificación de antecedentes para todos los empleados nuevos, especialmente para aquellos que tendrán acceso a información crítica. Esto puede incluir la revisión de historiales de empleo, antecedentes penales y referencias, siempre con base a las normas legales

que permite la ley del trabajo. Durante la selección el personal de recurso humano del PSC AUTHENTICSING deberá realizar la revisión y verificación de antecedentes de los candidatos, esto 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. Para esto se verificaran:

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

10.2.3 Capacitación y concienciación.

Es importante educar a los empleados sobre la importancia de la seguridad de la información y cómo pueden contribuir a mantenerla segura. Esto puede incluir la realización de capacitaciones, la difusión de políticas claras y la realización de simulaciones de ataques y pruebas de penetración.

En PSC AUTHENTHICSING promoverá la formación de su personal, tanto desde un aspecto técnico como conductual, fomentando una cultura de cumplimiento, la igualdad de oportunidades, la correcta capacitación técnica adaptadas a las necesidades específicas a través de la detección de carencias profesionales en función de una matriz de cualificaciones para cada puesto de trabajo, así como un plan de desarrollo de habilidades basado en la comunicación y mutua confianza entre cada empleado y su superior jerárquico.

Los directivos y empleados del PSC AUTHENTHICSING se comprometerán a actualizar permanentemente sus conocimientos técnicos y de gestión para desarrollar sus competencias, y a cumplir con los principios y valores de Authenticsing, realizando las acciones formativas asignadas a través de los planes de formación que facilita la Entidad, con objeto de favorecer su desarrollo profesional y aportar valor a los destinatarios de los productos y servicios.

10.2.4 Control de acceso y autorización.

Se deben implementar controles de acceso y autorización apropiados para limitar el acceso a la información crítica solo a aquellos empleados que lo necesiten para realizar sus funciones.

10.2.5 Detección y prevención de la fuga de información.

Se deben implementar medidas para detectar y prevenir la fuga de

información, como la monitorización del tráfico de red y el seguimiento de la información que se mueve dentro y fuera de la organización.

Con el fin de lograr cumplir la normativa interna del PSC AUTHENTICSING, las leyes y regulaciones aplicables y la seguridad de sus empleados, el PSC AUTHENTICSING se reserva el derecho a inspeccionar en cualquier momento y llevar un seguimiento de todos los sistemas informáticas del PSC AUTHENTICSING y de su plataforma tecnológica.

Los sistemas informáticos sujetos a inspección incluyen, pero no se limitan, a los archivos de sistema de correo electrónico, archivos del disco duro de ordenadores personales, archivos de buzón de voz, colas de impresión, documentación obtenida del fax, cajones del escritorio y áreas de almacenado. Estas inspecciones se llevarán a cabo tras haber sido aprobadas por el departamento de asesoría legal, con los procedimientos establecidos en la normativa legal aplicable, además el PSC AUTHENTICSING se reserva el derecho de eliminar de sus sistemas informáticos cualquier material que considere ofensivo o potencialmente ilegal o fraudulento.

10.2.6 Gestión de salidas.

Es importante tener un proceso claro y bien definido para la gestión de salidas de empleados, que incluya la desactivación de las cuentas de acceso y la eliminación del acceso a la información crítica.

10.2.7 Auditoría y revisión continúa.

La seguridad ligada a los recursos humanos debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.3 GESTIÓN 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 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. A continuación, se presenta un plan general para la gestión de activos:

10.3.1 Identificación de activos.

Se debe identificar todos los activos de la organización, incluyendo hardware, software, datos e información crítica, y establecer un inventario de los mismos.

- Inventario de activos: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
- Propiedad de los activos: Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
- Uso aceptable de los activos: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
- Devolución de activos: Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.

10.3.2 Evaluación de riesgos.

Se debe realizar una evaluación de riesgos de los activos identificados, para determinar los posibles peligros que enfrentan los activos y establecer medidas para mitigarlos.

10.3.3 Implementación de controles de seguridad.

Una vez identificadas las amenazas, se deben implementar controles de seguridad apropiados para proteger los activos críticos. Esto puede incluir la implementación de firewalls, antivirus, sistemas de autenticación y autorización, y políticas de acceso a la información.

10.3.4 Monitoreo y mantenimiento.

Es importante monitorear y mantener los activos de la organización de manera regular, para asegurarse de que estén actualizados y funcionando correctamente. Esto puede incluir la realización de mantenimiento preventivo y la aplicación de parches de seguridad.

10.3.5 Asignación y reasignación de activos.

Se debe tener un proceso claro para asignar y reasignar los activos de la organización, y asegurarse de que los empleados que los utilizan estén capacitados adecuadamente para hacerlo.

10.3.6 Gestión del ciclo de vida de los activos.

Los activos tienen un ciclo de vida, desde su adquisición hasta su eliminación. Es importante tener un proceso claro para la gestión del ciclo de vida de los activos, que incluya la planificación, adquisición, uso, mantenimiento y eliminación adecuada de los activos.

10.3.7 Auditoría y revisión continúa.

La gestión de activos debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.4 CONTROL DEL ACCESO.

El objetivo es establecer requisitos mínimos que están orientadas para controlar y monitorizar el acceso a los medios de información del PSC AUTHENTICSING por medio de sus redes, sistemas y aplicaciones, de acuerdos a las políticas definidas por Authenticsing. Es por esto que, EL PSC AUTHENTICSING dispone de procedimientos de control físico, lógico, de personal, y de operación, destinados a garantizar la seguridad necesaria en la gestión de los Certificados. Asimismo el PSC AUTHENTICSING registrara todos aquellos eventos relacionados con sus servicios que puedan ser relevantes con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad se desarrollan de conformidad con la normativa aplicable para poder determinar las causas de una anomalía detectada. A continuación, se presenta un plan general para un control de acceso efectivo:

10.4.1 Identificación de usuarios y roles.

Se debe identificar a los usuarios y los roles que tienen dentro de la organización, para determinar quiénes necesitan acceso a qué sistemas y datos.

Administrar de niveles de acceso privilegiado, desde el más alto y más estricto hasta el nivel básico de seguridad. La asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy

estricta, dados los derechos adicionales que generalmente se transmiten sobre los activos de información y los sistemas que los controlan.

10.4.2 Autenticación y autorización.

Se deben implementar medidas de autenticación y autorización apropiadas para garantizar que solo los usuarios autorizados puedan acceder a los sistemas y datos críticos.

10.4.3 Implementación de controles de seguridad.

Es importante implementar controles de seguridad adecuados, como firewalls, antivirus y sistemas de detección de intrusiones, para proteger los sistemas y datos críticos de AUTHENTICSING.

10.4.4 Monitoreo y registro de acceso.

Se debe monitorear y registrar el acceso a los sistemas y datos críticos del PSC AUTHENTICSING para detectar cualquier actividad sospechosa o no autorizada.

10.4.5 Gestión de contraseñas.

Se deben establecer políticas claras para la gestión de contraseñas, incluyendo la complejidad de las contraseñas y la frecuencia de su cambio.

10.4.6 Capacitación y concientización.

Es importante educar a los usuarios sobre la importancia de la seguridad de la información y cómo pueden contribuir a mantenerla segura, por ejemplo, mediante la elección de contraseñas seguras y la protección de sus credenciales de acceso.

10.4.7 Auditoría y revisión continúa.

El control de acceso debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.5 CONTROLES CRIPTOGRÁFICOS.

Un plan de política de los controles criptográficos es el conjunto de medidas y

procedimientos que se establecen para garantizar la protección de la información mediante el uso de técnicas de cifrado y descifrado de la información, a través de los controles criptográficos.

A continuación, se describen algunos elementos que se pueden incluir en un plan de política de los controles criptográficos:

10.5.1 Identificación de los datos críticos

Se debe identificar los datos críticos de la organización que necesitan ser protegidos mediante el uso de técnicas criptográficas.

10.5.2 Selección de algoritmos criptográficos

Se deben seleccionar los algoritmos criptográficos adecuados para proteger los datos críticos, teniendo en cuenta factores como la fortaleza del algoritmo, la compatibilidad con los sistemas existentes y los requisitos de rendimiento.

10.5.3 Gestión de claves

Se debe establecer una política clara para la gestión de claves criptográficas, que incluya la generación de claves aleatorias, la distribución segura de las mismas y la rotación periódica de las claves.

10.5.4 Implementación de controles de seguridad

Se deben implementar controles de seguridad adecuados, como firewalls, sistemas de detección de intrusiones y monitoreo de la actividad de red, para proteger los datos criptográficos.

10.5.5 Capacitación y concientización.

Es importante educar a los usuarios sobre la importancia de la seguridad criptográfica y cómo pueden contribuir a mantenerla segura, por ejemplo, mediante la protección adecuada de las claves criptográficas.

10.5.6 Uso de certificados digitales.

Se deben establecer medidas adecuadas para el uso de certificados digitales, para garantizar la autenticidad y la integridad de la información transmitida.

10.5.7 Seguridad de los procesos de cifrado.

Se deben establecer medidas adecuadas para garantizar la seguridad de los procesos de cifrado y descifrado de la información, para evitar posibles vulnerabilidades o brechas de seguridad.

10.5.8 Gestión de riesgos.

Se deben establecer medidas adecuadas para la gestión de riesgos relacionados con el uso de algoritmos criptográficos, para garantizar que se identifiquen y se mitiguen los riesgos potenciales.

10.5.9 Auditoría y revisión continua.

El control criptográfico debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.5.10 Cumplimiento normativo.

Se deben cumplir con las normativas y regulaciones aplicables, como la Ley de Protección de Datos Personales, el Reglamento General de Protección de Datos y otras regulaciones de privacidad que puedan aplicarse.

10.6 SEGURIDAD FÍSICA Y DEL AMBIENTE.

La seguridad física y del ambiente es un aspecto crítico de la seguridad de la información, ya que protege los activos físicos y ambientales de la organización que son necesarios para el funcionamiento de los sistemas y la infraestructura. A continuación, se presenta un plan general para la seguridad física y del ambiente:

10.6.1 Identificación de los activos físicos y ambientales críticos.

Se deben identificar los activos físicos y ambientales críticos de la organización, tales como servidores, dispositivos de almacenamiento, aire acondicionado, sistemas eléctricos y de iluminación, y establecer un inventario de los mismos.

10.6.2 Evaluación de riesgos.

Se debe realizar una evaluación de riesgos de los activos identificados, para determinar los posibles peligros que enfrentan los activos y establecer medidas para mitigarlos.

10.6.3 Implementación de controles de acceso físico.

Se deben implementar medidas de control de acceso físico para limitar el acceso a los activos críticos solo a aquellos empleados que necesitan acceder a ellos.

10.6.4 Implementación de controles ambientales.

Se deben implementar controles ambientales adecuados, como sistemas de control de temperatura, ventilación y humedad, para proteger los activos críticos de la organización.

10.6.5 Monitoreo y mantenimiento.

Es importante monitorear y mantener los activos físicos y ambientales de la organización de manera regular, para asegurarse de que estén actualizados y funcionando correctamente. Esto puede incluir la realización de mantenimiento preventivo y la aplicación de parches de seguridad.

10.6.6 Capacitación y concientización.

Es importante educar a los empleados sobre la importancia de la seguridad física y del ambiente y cómo pueden contribuir a mantenerla segura, por ejemplo, mediante la protección adecuada de los activos físicos y la notificación oportuna de cualquier problema ambiental.

10.6.7 Auditoría y revisión continúa.

La seguridad física y del ambiente debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.7 SEGURIDAD DE LAS OPERACIONES.

Objetivo: Asegurar la correcta operación en las instalaciones de procesamiento de información ya que se encarga de garantizar que los sistemas y procesos del PSC AUTHENTICSING estén protegidos contra posibles amenazas y riesgos. A continuación, se presenta un plan general para la seguridad de las operaciones:

10.7.1 Identificación de los sistemas críticos.

Se deben identificar los sistemas críticos de la organización, aquellos que son esenciales para la continuidad del negocio y que deben estar protegidos

de manera especial.

10.7.2 Evaluación de riesgos.

Se debe realizar una evaluación de riesgos para los sistemas críticos identificados, para determinar los posibles peligros que enfrentan los sistemas y establecer medidas para mitigarlos.

10.7.3 Implementación de controles de acceso.

Se deben implementar medidas de control de acceso adecuadas para limitar el acceso a los sistemas críticos solo a aquellos empleados que necesitan acceder a ellos.

10.7.4 Implementación de controles de seguridad.

Se deben implementar controles de seguridad adecuados, como firewalls, sistemas de detección de intrusiones y monitoreo de la actividad de red, para proteger los sistemas críticos de la organización.

10.7.5 Monitoreo y registro de actividad.

Es importante monitorear y registrar la actividad en los sistemas críticos de la organización, para detectar cualquier actividad sospechosa o no autorizada.

10.7.6 Gestión de parches y actualizaciones.

Se debe establecer una política clara para la gestión de parches y actualizaciones de software, que incluya la instalación de parches de seguridad y actualizaciones del sistema operativo de manera regular para garantizar que los sistemas estén actualizados y protegidos contra nuevas amenazas.

10.7.7 Capacitación y concientización.

Es importante educar a los empleados sobre la importancia de la seguridad de las operaciones y cómo pueden contribuir a mantenerla segura, por ejemplo, mediante la protección adecuada de las credenciales de acceso y la notificación oportuna de cualquier actividad sospechosa.

10.7.8 Auditoría y revisión continua.

La seguridad de las operaciones debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y

estén actualizados.

10.8 Gestión de las comunicaciones.

Para el PSC AUTHENTICSING tiene como objetivo en la gestión de la seguridad de la red es de garantizar la protección de los sistemas de red y de la información que circula a través de ellos, frente a posibles amenazas y vulnerabilidades. Es por esto que el PSC AUTHENTICSING implementa medidas de seguridad técnica y organizativa que permitan prevenir, detectar y responder de manera eficaz a los incidentes de seguridad que puedan afectar a la red y a los sistemas de la plataforma tecnológica que conforma al PSC AUTHENTICSING. A continuación, se presenta un plan general para la gestión de las comunicaciones:

10.8.1 Identificación de las comunicaciones críticas.

Se deben identificar las comunicaciones críticas del PSC AUTHENTICSING, aquellas que son esenciales para la continuidad del negocio y que deben estar protegidas de manera especial.

10.8.2 Evaluación de riesgos.

Se debe realizar una evaluación de riesgos para las comunicaciones críticas identificadas, para determinar los posibles peligros que enfrentan las comunicaciones y establecer medidas para mitigarlos.

10.8.3 Implementación de controles de acceso.

Se deben implementar medidas de control de acceso adecuadas para limitar el acceso a las comunicaciones críticas solo a aquellos empleados que necesitan acceder a ellas.

10.8.4 Implementación de controles de seguridad.

Se deben implementar controles de seguridad adecuados, como la encriptación de datos, la autenticación de usuarios y la verificación de integridad de los mensajes, para proteger las comunicaciones críticas de la organización.

10.8.5 Monitoreo y registro de comunicaciones.

Es importante monitorear y registrar las comunicaciones críticas el PSC AUTHENTICSING, para detectar cualquier actividad sospechosa o no autorizada.

10.8.6 Gestión de parches y actualizaciones.

Se debe establecer una política clara para la gestión de parches y actualizaciones de software de los sistemas de comunicaciones, que incluya la instalación de parches de seguridad y actualizaciones del sistema operativo de manera regular para garantizar que los sistemas estén actualizados y protegidos contra nuevas amenazas.

10.8.7 Capacitación y concientización.

Es importante educar a los empleados sobre la importancia de la seguridad de las comunicaciones y cómo pueden contribuir a mantenerla segura, por ejemplo, mediante el uso adecuado de las credenciales de acceso y la notificación oportuna de cualquier actividad sospechosa.

10.8.8 Auditoría y revisión continúa.

La gestión de las comunicaciones debe ser un proceso continuo, por lo que es importante realizar auditorías y revisiones regulares de los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

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

La gestión y continuidad del negocio es un aspecto crítico de la seguridad de la información, ya que se encarga de garantizar que la organización pueda seguir operando en caso de interrupciones o desastres. A continuación, se presenta un plan general para la gestión y continuidad del negocio:

10.9.1 Identificación de los procesos críticos.

Se deben identificar los procesos críticos del PSC AUTHENTICSING, aquellos que son esenciales para la continuidad del negocio y que deben estar protegidos de manera especial.

Tal es el caso de la plataforma tecnológica de AUTHENTICSING. Su centro de datos en DaycoHost, y sus operaciones en la sede administrativa del PSC AUTHENTICSING, incluido su enlace de comunicación entre la sede adminstrativa y el data center.

10.9.2 Evaluación de riesgos.

Se debe realizar una evaluación de riesgos para los procesos críticos identificados, para determinar los posibles peligros que enfrentan el PSC

AUTHENTICSING y establecer medidas para mitigarlos.

Es importante tener en cuenta que, además de las evaluaciones anuales, se deben realizar evaluaciones adicionales después de cualquier cambio significativo que se realicen en el PSC AUTHENTICSING o en su entorno, como la introducción de nuevos sistemas o procesos, la adquisición de nuevos equipos tecnológicos o la expansión de nuevos certificados.

Además, se recomienda realizar pruebas de continuidad del negocio al menos una vez al año para garantizar que el plan de continuidad del negocio sea efectivo y esté actualizado. Estas pruebas deben incluir una variedad de escenarios de interrupción o desastres para garantizar que el plan de continuidad del negocio sea efectivo en una variedad de situaciones.

10.9.3 Implementación de medidas de protección.

Se deben implementar medidas de protección adecuadas para garantizar la disponibilidad de los procesos críticos en caso de interrupciones o desastres, como la implementación de sistemas de respaldo y redundancia.

10.9.4 Planificación de la continuidad del negocio.

Se debe desarrollar un plan de continuidad del negocio para garantizar que la organización pueda seguir operando en caso de interrupciones o desastres. Este plan debe incluir procedimientos para la recuperación de desastres, la implementación de sistemas de respaldo, la identificación de áreas de trabajo alternativas y la comunicación con los clientes y proveedores.

10.9.5 Pruebas y mantenimiento.

Es importante realizar pruebas regulares en la plataforma tecnológica del PSC AUTHENTICSING del plan de continuidad del negocio para asegurarse de que esté actualizado y sea efectivo. También se deben realizar mantenimientos regulares de los sistemas de respaldo y redundancia para garantizar su correcto funcionamiento.

10.9.6 Capacitación y concientización.

Es importante educar a los empleados del PSC AUTHENTICSING sobre la importancia de la gestión y continuidad del negocio y cómo pueden contribuir a mantenerla segura, por ejemplo, mediante la protección adecuada de los datos y recursos críticos y la notificación oportuna de cualquier problema.

10.9.7 Auditoría y revisión continúa.

La gestión y continuidad del negocio debe ser un proceso continuo en el PSC AUTHENTICSING, por lo que es importante realizar auditorías y revisiones regulares del plan de continuidad del negocio y los controles de seguridad implementados para asegurarse de que sigan siendo efectivos y estén actualizados.

10.10 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.

10.10.1 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.

10.10.2 Implementación de la continuidad de la seguridad de la información.

10.10.2.1 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.

10.10.2.2 Funciones.

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

10.10.2.3 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.”

10.10.3 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

11. ACCESO FISICO.

El PSC AUTHENTICSING garantiza que cumple la normativa aplicable en todos los aspectos de seguridad física y las describe a continuación.

11.1 UBICACIONES DE LAS INSTALACIONES.

11.1.1 Oficina administrativa.

Los controles de acceso físico aplicados a la oficina administrativa de AUTHENTICSING contemplarán la seguridad en la gestión del ciclo de vida de los certificados y la seguridad física de la sede y de los equipos de computación y demás componentes informáticos localizados dentro de la referida sede administrativa.

11.1.1.1 Zona 1.

La gestión del ciclo de vida de los certificados es un proceso crítico para la seguridad y confiabilidad de los sistemas de cifrado y autenticación en el PSC AUTHENTICSING. Todos los procesos de gestión del ciclo de vida de los certificados son llevados a cabo en la sede administrativa de Authenticsing, en áreas asignadas al operador del AR y AC, donde el cliente solo tendrá acceso para el proceso de generación del par de clave en la fecha prevista por el operador AR en previa cita con el cliente.

- Generación del certificado: en primer lugar, se crea el certificado, que incluye una clave pública y privada con la identidad del titular del certificado. El certificado se crea utilizando un algoritmo de cifrado asimétrico, ECDSA-whit - SHA-384 de curva elíptica.
- Firma del certificado: el certificado se firma digitalmente utilizando la clave privada del signatario del certificado. Esta firma digital garantiza la autenticidad del certificado y su integridad.
- Distribución del certificado: una vez generado y firmado el certificado, se distribuye a los sistemas y usuarios que necesitan utilizarlo para cifrar o autenticar la información.
- Uso del certificado: el uso de los certificados electrónicos generados y emitidos por el PSC AUTHENTICSING cumple con las leyes y regulaciones aplicables y estará limitado para cada uno de los diferentes tipos de certificados electrónicos que son emitidos por el PSC AUTHENTICSING.
- Renovación del certificado: los certificados tienen una fecha de

expiración, por lo que es necesario renovarlos antes de que caduquen. Bajo las presentes Políticas de Certificación, el PSC AUTHENTICSIG la renovación del certificado implica generar un nuevo certificado con una nueva fecha de expiración y firmarlo digitalmente.

- Revocación del certificado: en caso de que se sospeche que un certificado ha sido comprometido o que ya no es válido por alguna razón, se debe revocar el certificado. La revocación del certificado implica agregar una entrada de revocación a la lista de certificados revocados (LCR) o a un servicio de validación de certificados (OCSP, por sus siglas en inglés).
- Eliminación del certificado: una vez que un certificado ha expirado o ha sido revocado, se debe eliminar de los sistemas y usuarios que lo han utilizado.

Es importante mencionar que la gestión del ciclo de vida de los certificados es un proceso continuo y en constante evolución. Los certificados deben ser gestionados de manera adecuada para garantizar que la información se cifre y autentique de manera segura y confiable.

11.1.1.2 Zona 2.

La protección física de esta zona se implementa a través de la creación de perímetros de seguridad claramente definidos (es decir, barreras físicas), por tal sentido y como política de seguridad no está permitido compartir esta áreas del PSC AUTHENCSIN con otras organización o actividad ajena a la que está destinada esta zona. Todo acceso del personal autorizado debe quedar registrado y debe contar con al menos un (1) factor de seguridad (tarjeta electrónica, biometría y/o clave).

- La seguridad física de la sede administrativa del PSC AUTHENTICSING contará con la vigilancia de acceso al edificio donde se encuentra ubicada, luego de las 6:00 p.m. hasta las 6:00 a.m. del día próximo de lunes a viernes de cada semana y de cada mes. Los fines de semana y días feriados, el acceso al edificio donde se encuentra localizada la sede administrativa se encuentra restringido, debiendo ser identificada toda persona que ingrese a la torre empresarial tanto en su ingreso como en su egreso. El retiro de equipos y componentes se encuentra restringido en todo momento y requiere de la presentación de una autorización a tales efectos.
- El pasillo de acceso a la sede física de AUTHENTICSING contará

con una vigilancia adicional a través de un sistema de cámaras digitales.

- El acceso a la sede administrativa contará con un doble mecanismo físico de protección el cual comprende:
  - Intercomunicador
  - Reja blindada de seguridad con triple anclaje y cerradura reforzada;
  - Se ejecutará un sistema de alarma con sirena que emite una señal audible al activarse, teclado que permite desmontar y el sistema por medio de una clave de usuario, sensores de movimientos, con batería de respaldo de hasta 8 horas en caso de corte de corriente.
  - Se contratará un servicio de protección con respuesta rápida las 24 horas al día, según las eventualidades de seguridad.

11.1.2 Tercerización (subcontratados).

Para el caso de los servicios tercerizados (subcontratados), como es el caso de DaycoHost, el PSC AUTHENTICSING se acogerá a las políticas de seguridad de la información establecida por el proveedor de servicio; para este caso el PSC AUTHENTICSING ha suscrito contrato con DaycoHost donde se alojan los servidores y equipos de comunicación del PSC AUTHENTICSING y donde están aislado, garantizando la integrad, confiabilidad, accesibilidad a los servicios.

11.1.2.1 Zona 2.

A continuación, se presentarán los Servicios tercerizados que contratará el PSC AUTHENTICSING**:**

- Centro de datos (housing), empresa Daycohost.
  - Acceso a múltiples proveedores de servicio de conectividad del mercado.
  - Anclaje sismo resistente.
  - Climatización óptima.
  - Vigilancia 7x24x365.
  - Alimentación eléctrica equivalente a 1,5 KVA.
  - Seguridad (física).
  - Sistema de energía con UPS.
  - Infraestructura en redundancia N+1.
  - Alimentación eléctrica a doble barra, con aterramiento individual.

Esto aplica para el Data center ubicado en la ciudad de Caracas y el data center ubicado en la ciudad de Valencia.

11.1.3 Centro de Datos

11.1.3.1 Controles de acceso físico.

El PSC AUTHENTICSING determinará como área critica para los servicios de certificación de firmas electrónicas el lugar donde se encuentran instalados los servidores de la plataforma de certificación, y establecerá los siguientes criterios con el fin de permitir solo al personal autorizado en acceso físico a esta área, con base a las políticas de seguridad de DaycoHost el cual se basa en las siguientes niveles de acceso:

- Al menos 7 capas para el acceso desde el exterior del centro de datos hasta el área de rack donde están instalados los servidores de la plataforma de certificación.
- Servicio de vigilancia con personal armado 24x7x365.
- Registro de las fechas y horas de ingreso y egreso de cada una de las personas que accedan al área de rack.
- Utilización de cámaras de seguridad en las instalaciones del centro de datos.
- Inclusión en las capas de seguridad al menos 1 control biométrico.
- El acceso físico para el interior del rack (apertura) deberá estar autorizado solo al personal del PSC AUTHENTICSING.

Daycohost como el proveedor del centro de datos, cumple con cada uno de los requisitos mínimos de controles de acceso físico contemplados en el presente plan y su política, los cuales se especifican a continuación:

- Cerca perimetral;
- Vigilancia con personal y cámaras digitales;
- Control de ingreso con vigilancia en el cerco perimetral del edificio del centro de datos
- Control de ingreso en la entrada al área interna del centro de datos
- Control de ingreso al pasillo de acceso al área de servidores con dispositivo biométrico sensible al calor e identidad
- Carnet de magnético de seguridad para puerta de acceso al área interna de control del área de servidores.
- Llave de acceso al rack de servidores;
- Cubierta de seguridad metálica con cerradura que impide el acceso

no autorizado al servidor de la AC. La descripción de los mencionados niveles es la siguiente:

- La vigilancia con personal y cámaras digitales comprende el servicio 7X24X365 días. En este nivel se registran los equipos portátiles de computación.
- La cerca perimetral limita el acceso físico a la sede del centro de datos.
- El control de ingreso con vigilancia en el cerco perimetral del edificio del centro de datos valida que solo nada más y menos que el equipo autorizado por el DE AUTHENTICSING ingrese a las instalaciones.
- El control de ingreso a la entrada del área interna del centro de datos se constituye en un mecanismo de doble aseguramiento de ingreso del personal autorizado, se validan las computadoras portátiles y se direcciona a la recepción principal para anunciar al personal autorizado para el acceso, el cual debe ser aceptado desde lo interno del área de servidores del centro de datos.
- El control de ingreso al pasillo de acceso al área de servidores se establece en un triple mecanismo de aseguramiento de acceso al área pública del centro de datos y al área de servidores. En este control solo se valida la identidad de la persona autorizada por el DE AUTHENTICSING para ingresar al área de servidores.
- El dispositivo biométrico sensible al calor e identidad tiene como objetivo bloquear el acceso al área de servidores para el personal no autorizado y acompañado por personal técnico y de operaciones.
- El carnet de magnético de seguridad para puerta de acceso al área interna de control del área de servidores verifica que en efecto sólo el personal autorizado y poseedor de la tarjeta cuente con acceso al área de control de servidores.
- El control de acceso al cuarto de servidores es realizado por los operadores de área de control externa del área de servidores. Los operadores verifican la identidad de la persona que ingresará al área de servidores, luego registra sus datos como la hora de ingreso y egreso.
- La llave de acceso al rack de servidores de AUTHENTICSING deberá estar en posesión del personal de AUTHENTICSING para garantizar la seguridad y custodia de los servidores y de la Autoridad de Certificación (AC).
- El funcionamiento de seguridad del ingreso a la puerta del rack de servidores de AUTHENTICSING se constituye en el sistema de seguridad que permite que sólo los operadores de AUTHENTICSING podrán acceder a los servidores de la

plataforma de certificación.

- La protección o cubierta metálica del servidor de la CA que posee cerradura, limitando de esta manera el acceso al servidor de la CA, solo al personal autorizado por la Alta Dirección de AUTHENTICSING

El personal de AUTHENTICSING comprobará, revisará y auditará cada control de seguridad aplicados por el centro de datos regularmente, con el fin de garantizar y asegurar el correcto cumplimiento de los mismos.

11.1.3.2 Zona 3.

Los controles de seguridad física y ambiental se aplicarán para proteger los sistemas y las instalaciones, por lo que se deberán tener controles de protección contra desastres naturales, controles de seguridad contra incendios, controles ante fallas de servicios públicos (por ejemplo, energía, telecomunicaciones), colapso de la estructura, fugas en las tuberías, protección contra el robo, allanamiento de las instalaciones, etc.

11.1.3.2.1 Suministro de energía

Los servidores de la plataforma de certificación contará con una alimentación garantizada por el centro de datos de un 99,9%, el suministro de energía contar con:

- Múltiples enchufes y líneas de suministro.
- Servicio de energía ininterrumpido (UPS) principal y de respaldo.
- Generador principal y generador secundario, como respaldo de los UPS.

AUTHENTICSING solicitará a la empresa Daycohost una constancia de cada uno de los mantenimientos preventivos y correctivos realizados para los equipos que conforman el sistema de energía del centro de datos.

11.1.3.2.2 Seguridad del cableado

Cada cableado del centro de datos, incluyendo la conexión que va desde el rack de AUTHENTICSING hasta todos los equipos que ofrecen el servicio de internet, estará protegido de la manera siguiente:

- Las escalerillas de datos y de energía separadas.
- Todos los cables debidamente identificados en sus extremos.
- El cableado utilizado será categoría 6E y certificado por panduit.
- El área de switch de backbone estará restringida, solo el personal autorizado de Daycohost tiene acceso.
- La manipulación del cableado será realizada solo por personal altamente capacitado de Daycohost.

El cableado de la red interna (LAN) de la plataforma de certificación será manipulada solo por el equipo especializado de AUTHENTICSING y también contará con un respaldo en caso de ruptura o falla de alguno de los patch cord instalados.

11.1.3.2.3 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:

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

Entre internet y la PRIMERA ZONA, solo estarán permitidas las conexiones mínimas requeridas para el acceso a los servicios de certificación que ofrece al PSC AUTHENOLOGY. Entre la PRIMERA ZONA y la SEGUNDA ZONA, solo se permitirán las conexiones mínimas necesarias para la operación de la plataforma de certificación. Y para las funcionalidades de firewall, el equipo de seguridad instalado solo tendrá habilitado las siguientes funciones: IDS/IPS y Antivirus.

12. ACCESO LÓGICO A LOS SISTEMAS.

El PSC AUTHENTICSING llevará a cabo controles para proteger los equipos, información, medios de comunicación y el software relacionado con la Servicios de la AC. El PSC AUTHENTICSING se asegurará de que el acceso al sistema se

limita a las personas debidamente autorizadas. Quedando registrado los accesos y actividades en los sistemas, el cual se habilitara los logs de auditorías en base de datos y servicios relacionados. Los mismos deben resguardarse como parte de la política de respaldo. El PSC AUTHENTICSING cuenta con firewall para evitar accesos no autorizados dentro de las operaciones de la AC

- Los datos sensibles estarán protegidos contra el acceso o modificación no autorizada, solo pudendo acceder el personal autorizado para consultar, monitorear o manipular. Solo se permitirán conexiones por VPN para el intercambio de información de datos sensibles para interconexiones las redes de la sede administrativa y el Data Center. Para esto quedara un registro en logs.
- La AC se asegurara una gestión eficaz del usuario para mantener la seguridad del sistema, esto incluye la gestión de cuentas de usuario, auditoría y la modificación puntual o eliminación del acceso en caso de ser necesario.
- La AC garantiza que el acceso a la información, sistemas o aplicaciones están restringidas de acuerdo con la política de control de acceso y controles de seguridad informática suficientes para la separación de funciones según los roles identificados en las prácticas de AC, esto incluye el administrador de seguridad y operación. En particular, el uso de programas o aplicaciones estará restringido y estrechamente controlado. Se limitará sólo a permitir el acceso a los recursos necesarios para llevar a cabo las funciones asignadas al usuario correspondiente.
- Como parte de las políticas el personal de la AC deberá estar identificado y autenticado antes de utilizar aplicaciones críticas relacionadas con la gestión de certificados.
- El personal de la AC deberá rendir cuentas de sus actividades, esto se dará mediante los registros de eventos.
- Los datos sensibles estarán protegidos de usuarios no autorizados, en caso de ser revelados a través de objetos de almacenamiento reutilizados (por ejemplo archivos borrados), se realizara una evaluación de seguridad para determinar la falla del proceso y se elevara el caso a la alta gerencia el cual determinar el procedimiento jurídico o legal.

12.1 CONTROL DE ACCESO.

12.1.1 Identificación y autenticación.

Todos los usuarios que accedan a los sistemas que conforma la plataforma tecnológica del PSC AUTHENTICSING deben ser identificados y autenticados antes de permitirles el acceso. Esto puede incluir el uso de contraseñas fuertes, autenticación multifactorial y otras medidas de seguridad para garantizar que solo las personas autorizadas tengan acceso

a los sistemas.

12.1.2 Control de acceso.

Para garantizar que solos los usuarios autorizados tengan acceso a las funciones y datos necesarios para realizar sus tareas y actividades en las que están autorizados y tengan acceso a las funciones y datos necesarios para realizar sus tareas. Todos y cada uno de los usuarios que trabajan en el PSC AUTHENTICSING tienen definidos sus responsabilidades y roles en la organización y el administrador de tecnología asignara los permisos y control de acceso basado en roles.

12.1.3 Monitoreo de acceso.

Se deben establecer medidas de monitoreo para detectar y registrar cualquier acceso no autorizado o intentos de acceso a los sistemas de la PKI. Esto puede incluir la revisión de registros de acceso, la detección de patrones de acceso sospechosos y el monitoreo de la actividad de los usuarios.

12.1.4 Auditoría de acceso.

Authenticsing debe realizar auditorías periódicas del acceso a los sistemas de tecnológica del PSC AUTHENTICSING para asegurarse de que se cumplan las políticas y los controles de acceso establecidos y para identificar cualquier acceso no autorizado o comportamiento sospechoso.

Los sistemas de archivos utilizados por el PSC AUTHENTICSING para conservar estos registros auditados, serán los internos propios de la infraestructura, y además se utilizarán soportes externos con capacidad de almacenamiento durante largos periodos de tiempo. Estos soportes tendrán las garantías suficientes para impedir que los registros sufran cualquier tipo de alteración.

EL PSC AUTHENTICSING realizará varias copias que se almacenarán en diferentes lugares, que dispondrán de todas las medidas de seguridad física y lógica que eviten, en lo que razonablemente sea posible, una alteración del soporte almacenado y de los datos que contenga estos soportes.

Este archivo está provisto de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación de los certificados y eventos almacenados.

12.1.5 Capacitación de los usuarios

Es importante capacitar a los usuarios sobre las mejores prácticas de seguridad de la información y sobre las políticas y procedimientos de acceso a los sistemas que conforma la plataforma tecnológica del PSC AUTHENTICSING. Los usuarios deben estar al tanto de los riesgos de seguridad de la información y capacitados para manejar la información de manera segura.

13. IMPLEMENTACIÓN DEL SISTEMA DE CONFIANZA Y MANTENIMIENTO.

El sistema de la AC del PSC AUTHENTICSING debe asegurarse de usar sistemas y productos que aseguren la protección a alteraciones. Es por esto que la implementación de un Sistema de Confianza y Mantenimiento (SCM) para una Autoridad de Certificación (AC) el cual es un proceso importante para garantizar la confianza y la seguridad en los certificados que emite la AC con respecto a su plataforma tecnológica.

13.1.1 Análisis de los requisitos de seguridad

Un análisis de los requisitos de seguridad se llevará a cabo en la etapa de diseño y la especificación de los requisitos de cualquier proyecto de desarrollo de sistemas realizado para la AC o en nombre de la AC para garantizar la seguridad del proceso. A continuación, se describen los principales pasos que se deben seguir para implementar un sistema de confianza y mantenimiento la AC en la plataforma tecnológica del PSC AUTHENTICSING:

- **Ddefinir los requisitos:** se deben definir los requisitos la plataforma tecnológica, esto incluyendo la gestión de claves, la renovación y revocación de certificados, la gestión de políticas y procedimientos, entre otros aspectos importantes.
- **Diseñar la arquitectura:** se debe diseñar la arquitectura de la plataforma tecnológica, incluyendo los componentes de software y hardware necesarios para implementar los requisitos definidos en el paso anterior.
- **Implementar el software:** una vez diseñada la arquitectura de la plataforma tecnológica, se debe implementar el software necesario para gestionar los certificados, las claves y los procesos de renovación y revocación de los certificados.
- **Configurar las políticas y procedimientos**: se deben definir y configurar las políticas y procedimientos necesarios para la gestión de los

certificados, incluyendo el proceso de emisión, renovación y revocación de certificados, la gestión de claves, entre otros aspectos importantes.

- **Realizar pruebas y validación:** se deben realizar pruebas y validaciones exhaustivas de la plataforma tecnológica antes de ponerlo en producción, para garantizar que funciona correctamente y cumple con los requisitos definidos.
- **Puesta en producción:** una vez que se han completado las pruebas y validaciones, se puede poner en producción de la plataforma tecnológica y comenzar a emitir y gestionar los certificados de la AC.
- **Monitoreo y mantenimiento:** se deben establecer medidas de monitoreo y mantenimiento periódico de la plataforma tecnológica, para garantizar que sigue funcionando correctamente y cumpliendo con los requisitos definidos. Esto implica la revisión periódica de los registros y la realización de auditorías de seguridad.

La implementación de un Sistema de Confianza y Mantenimiento es un proceso crítico para garantizar la seguridad y la confianza de la plataforma tecnológica en los certificados emitidos por una AC. Es importante que este proceso se lleve a cabo de manera rigurosa y documentada, y que se realicen actualizaciones y revisiones periódicas para adaptarse a las nuevas amenazas y vulnerabilidades que puedan surgir.

13.1.2 Procedimientos de control de cambios

Debe existir un procedimiento de control de cambios para nuevas versiones, modificaciones y correcciones de software de operacional de la AC del PSC AUTHENTICSING.

Los procedimientos de control de cambios para nuevas versiones, modificaciones y correcciones de software operacional son un conjunto de medidas y procedimientos que se establecen para garantizar que los cambios realizados en el software operacional sean controlados y documentados adecuadamente. A continuación, se describen los principales pasos en el proceso de control de cambios:

- **Identificación del cambio:** en primer lugar, se debe identificar y documentar el cambio que se desea realizar en el software operacional. Esto puede ser una nueva versión, una modificación o una corrección.
- **Análisis de impacto:** a continuación, se debe realizar un análisis de impacto para determinar el impacto que tendría el cambio en el software operacional y en los sistemas que lo utilizan. Esto implica evaluar los riesgos y las posibles consecuencias del cambio.

- **Diseño y desarrollo:** una vez que se ha evaluado el impacto del cambio, se puede proceder al diseño y desarrollo del cambio en el software operacional. Esto puede implicar la creación de nuevo código, la modificación del código existente, o la integración de componentes de terceros.
- **Pruebas y validación:** se deben realizar pruebas exhaustivas del cambio para validar su funcionamiento y asegurarse de que no hay errores o problemas de compatibilidad con otros sistemas.
- **Documentación y aprobación:** una vez que se ha validado el cambio, se debe documentar adecuadamente el proceso y los resultados de las pruebas. Además, se debe obtener la aprobación de los responsables de la gestión de la seguridad y de los sistemas para proceder a la implementación del cambio.
- **Implementación y verificación**: se debe implementar el cambio en el software operacional y verificar que funciona correctamente. Es importante llevar un registro de la implementación y realizar una revisión posterior para asegurarse de que se han cumplido todos los procedimientos y que no se han producido errores o problemas.
- **Gestión de cambios:** se debe llevar un registro de todos los cambios realizados en el software operacional y mantener actualizada la documentación correspondiente. Además, se deben establecer medidas de monitoreo y mantenimiento periódico para garantizar que el software operacional sigue funcionando correctamente después de los cambios realizados.
- **Monitoreo y revisión de cambios:** Después de la implementación de cambios en el software operacional, se deben monitorear y revisar regularmente para asegurarse de que funcionan correctamente y no afectan la seguridad o la eficacia de la plataforma tecnológica del SPC AUTHENTICSING.

Es importante mencionar que los procedimientos de control de cambios deben formar parte de un marco más amplio de gestión de la seguridad de la información, que incluya políticas y procedimientos para la gestión de riesgos, la gestión de incidentes, la gestión de continuidad del negocio, entre otros aspectos fundamentales para garantizar la seguridad y la disponibilidad de los sistemas de información de la organización.

13.1.3 Mantenimiento para los equipos

Con el fin de limitar las posibilidades o probabilidades de alguna falla física de los equipos que conforman la plataforma de certificación del PSC AUTHENTICSING, se decretará un plan de mantenimiento preventivo que

contemple los equipos, la regularidad y las acciones o actividades de mantenimiento, Además, el PSC AUTHENTICSING desarrollará un plan de mantenimiento correctivo, el cual contemplará una lista de probables fallas típicas en cada una de las cuales se determinarán las acciones de precaución que se deben tomar. Los operadores de informática serán los encargados de ejecutar tanto los mantenimientos preventivos (según su regularidad) y los mantenimientos correctivos (según el acontecimiento) y la supervisión y aseguramiento de cumplimiento de dichas actividades será efectuada por el Consultor de Tecnología y el Gerente Principal a la ejecución de cada mantenimiento, los operadores tendrán que notificar al Consultor de Tecnología (entregando un breve informe) los detalles del mismo. El Consultor de Tecnología posteriormente informará al Gerente Principal.

13.1.4 Equipos averiados o reutilizados

Los operadores de informática destruirán físicamente todas aquellas unidades de almacenamiento averiadas, y adicionalmente, en caso de una reutilización de una unidad de almacenamiento (disco duro), la misma será formateada de forma segura. Posterior a la ejecución de la acción, los operadores deberán notificar al Consultor de Tecnología (entregando un breve informe) los detalles del mismo. El Consultor de Tecnología posteriormente informará al Gerente general.

13.1.5 Áreas y pantallas limpias

Cada uno de los empleados de la empresa será informado acerca de los lineamientos a seguir como política de áreas y pantallas limpias.

13.1.6 Retiro de activos

Todo retiro de equipo, información o software deberá estar aprobado formalmente por el Gerente General o un representante de la alta dirección.

14. NORMATIVA PARA EL CUMPLIMIENTO DEL PLAN

El cumplimiento de normativas es esencial para garantizar que el PSC AUTHENTICSING cumpla con los estándares y requisitos legales, reglamentarios y de mejores prácticas aplicables de acuerdo al marco normativo nacional establecido en la LSMDFE y su Reglamento, así como las normas SUSCERTE. El presente documento considera el plan de cada una de las acciones enunciadas en el documento de la política de seguridad de la información y señala las estructuras y acciones que necesitaran ser cumplidas para la debida ejecución y control de gestión, tanto de la política como del presente plan. Adicionalmente, el presente plan

describe los controles y procesos asociados a los desarrollos de seguridad, de modo que derivan del documento de la política de seguridad de la información y del análisis integral de riesgos y amenazas.

El cumplimiento de las normativas para el plan está sujeto a diferentes normativas. A continuación, se mencionan las normativas comunes que pueden aplicarse en el cumplimiento del plan:

- **Normativas legales:** El PSC AUTHENTICSING deberá garantizar que se cumplen todos los requisitos legales aplicables de acuerdo al marco normativo nacional establecido (LSMDFE y su Reglamento, así como las normas SUSCERTE de carácter sub legal y cualquier otro marco regulatorio relacionado, para la protección de pérdida, destrucción y/o falsificación de los registros. Algunos registros pueden necesitar ser retenidos de manera segura para cumplir con los requisitos legales.

- **Normativas internas:** El PSC AUTHENTICSING debe contar con normativas internas que establezcan políticas, procedimientos y directrices específicas para el desarrollo del plan. Estas normativas están relacionadas con la gestión de riesgos, gestión de la seguridad de la información, entre otros aspectos.

- **Normativas de estándares:** El PSC AUTHENTICSING aplica las diferentes normativas de estándares que son aplicadas en el desarrollo del plan, en el ámbito de la seguridad de la información, pueden aplicarse normativas como ISO 27001, ISO 27002, NIST SP 800-53ª o ETSI 102 042 V 2.4.1.

- **Normativas de mejores prácticas:** El PSC AUTHENTICSING aplicara las diferentes normativas de mejores prácticas que son aplicadas en el desarrollo del plan para la gestión de servicios de TI, tal es el caso normativas como ITIL o COBIT.

Es importante que se identifiquen y se cumplan todas las normativas que sean aplicables en el desarrollo del plan de la seguridad de la información, ya que permitirá garantizar su éxito y evitar posibles sanciones o incumplimientos legales. Además, es recomendable que se establezcan medidas de monitoreo y seguimiento para asegurar el cumplimiento continuo de las normativas y la mejora continua del plan en el tiempo.

15. APROBACIÓN Y MODIFICACIÓN.

Los procedimientos y medios asociados para la aprobación y modificación o ajuste de la documentación del PSC AUTHENTICSING serán regulados y organizados por el documento de la política de documentación y gestión documental

16. RESPONSABILIDADES Y FUNCIONES.

Las responsabilidades y funciones de los distintos niveles del PSC AUTHENTICSING en cuanto al uso, control y seguridad del actual documento, se encuentran explicados y definidos en el documento de la política para el establecimiento de funciones y responsabilidades.

--- Fin de Documento ---