MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE AREVALO S.A

TRABAJO FIN DE MASTER FASE 2

Control Documental

Versión	Autor	Fecha	Descripción
1.0	Gustavo Arévalo Arenas	Marzo 26 2013	Versión Inicial

Revisión del Documento

Nombre	Cargo	Versión	Fecha	Comentarios
Gustavo Arévalo Arenas	Gerente de Proyecto	1.0	Marzo 26 2013	Ninguno

Aprobación del Documento

Versión	Aprobación	Fecha	Descripción
Gustavo Arévalo Arenas	Gerente de Proyecto	Marzo 26 2013	Ninguno

CONTENIDO

1 PREFACIO (INTRODUCCION)

La información relacionada con los procesos de negocio de AREVALO S.A, es un activo de mucho valor para la organización, por lo tanto requiere una protección del uso no adecuado, de su publicación no autorizada, de robo, alteración o destrucción. Una gestión de seguridad de la información efectiva garantiza que pueda ser compartida mientras se minimiza su exposición al riesgo.

Cualquier que sea la forma que esta tome ó el medio por el cual es almacenada ó compartida, esta siempre debe ser apropiadamente protegida.

Este manual identifica estos elementos para la gestión de la seguridad de la Información de la Empresa AREVALO S.A, cuyo propósito fundamental es garantizar y propender por la integridad, disponibilidad y confidencialidad, de la seguridad de los sistemas de información y de los datos, definido con base en las directrices y políticas de la Dirección y los requisitos de las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005.

2 VISIÓN ESTRATÉGICA

2.1 Misión de AREVALO S.A

Garantizar la prestación de servicios de suministros de productos alimenticios de mar, con un alta estándar de calidad, buscando la satisfacción de nuestros clientes nacionales e internacionales.

2.2 Visión de AREVALO S.A

AREVALO S.A, en el 2018 será reconocida como la Empresa líder en la fabricación y producción de productos alimenticios en Colombia, basados en la prestación de servicios de calidad, con altos estándares internacionales.

3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.2 Principios del Sistema de Gestión Seguridad de la Información "SGSI"

Los principios de seguridad son la base sobre la que se ha definido el Sistema de Gestión de Seguridad de la Información.

- El SGSI soporta la estrategia de la organización.
- El SGSI es un elemento integral para la protección de activos.
- El SGSI debe soportarse en controles Costo-Efectivos.
- Todos los empleados, proveedores y clientes cuentan con una responsabilidad y hacen parte fundamental del SGSI.
- El SGSI debe mejorarse continuamente.

3.3 Compromiso de la Dirección

- Mantener un sistema de gestión de la Seguridad de la Información que garantice el cumplimiento de los objetivos de seguridad requerido para ejecutar los planes estratégicos y los procesos de negocio de AREVALO S.A.
- Garantizar y motivar la participación de todos los funcionarios de AREVALO S.A, proveedores y socios de negocios en el desarrollo del Sistema de Gestión de la Seguridad de la Información
- Mantener un nivel de protección sobre los riesgos que puedan afectar la seguridad de la información que crea, procesa y resguarda la Organización como parte de la debida diligencia de la Dirección.
- Proveer los recursos necesarios para garantizar el debido cuidado de la información que crea, procesa o resguarda la Organización.

3.4 Representante de la Dirección

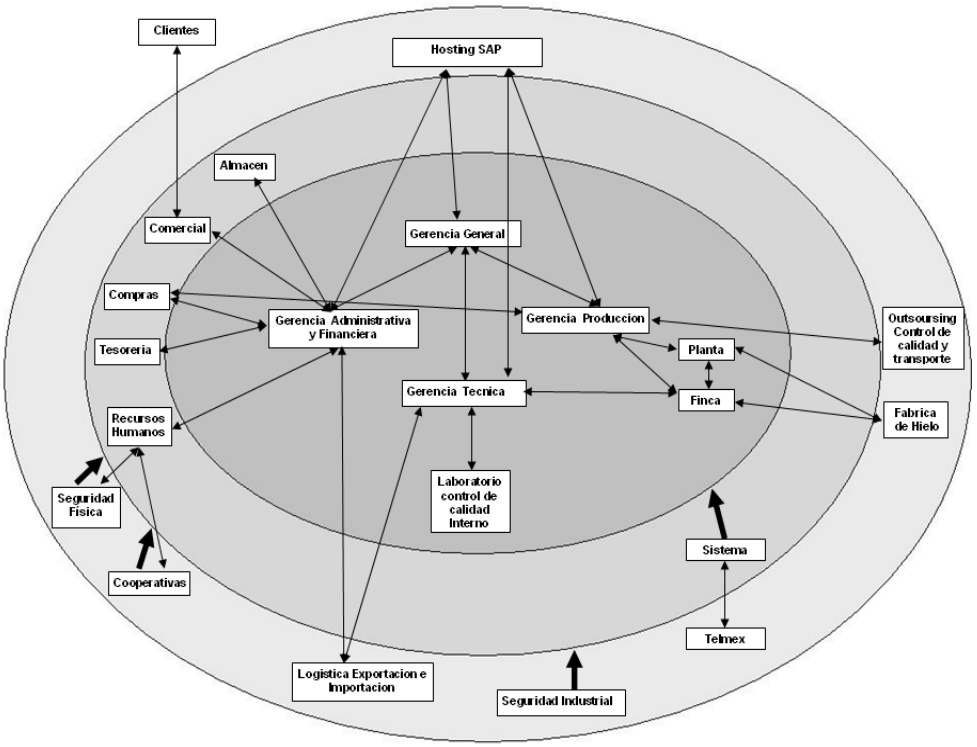
La Dirección ha designado a la firma UOC-MISTIC como LIDER del proceso de GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, basado en la figura de outsourcing, como su representante

frente al sistema de gestión de la seguridad de la información, con la responsabilidad y autoridad para:

- Asegurar que se promueva la toma de conciencia de la seguridad de la información en todos los niveles de la organización, proveedores y socios estratégicos.
- Asegurar que se establecen, implementan y mantienen los procesos necesarios para el sistema de gestión de la seguridad de la información.
- Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información y de cualquier necesidad de mejoramiento.
- Interactuar con partes externas sobre asuntos relacionados con el sistema de gestión de la seguridad de la información.

3.5 Alcance Del Sistema De Gestión De La Seguridad De La Información

El alcance del SGSI definido se presenta en la siguiente ilustración.



El SGSI tiene por alcance todos los procesos de AREVALO S.A (estratégico, misionales y soporte), incluyendo sus activos de información.

3.6 Exclusiones Del Sistema De Gestión De La Seguridad De La Información

El Sistema de Gestión de Seguridad de la Información de AREVALO S.A no excluye ningún numeral de la norma ISO 27001. Para las exclusiones de las mejores prácticas definidas en el estándar ISO 27002 remitirse a la Declaración de Aplicabilidad definida.

3.7 Políticas De Gestión De Seguridad De La Información

El objetivo del SGSI es el de proteger la información que crean, gestionan o resguardan los procesos de negocio con el fin de brindar protección social a través de la prestación de servicios acordes con la propuesta de valor ofrecida, mediante una mejora continua de la seguridad.

Con el fin de cumplir con el objetivo, la organización ha venido trabajando en el diseño de las políticas referentes a la seguridad de la información, las cuales se encuentran en el documento POL-AREVALO-01.

Se deben anexar al contrato de trabajo la aceptación por parte de todos los funcionarios de la organización y a los proveedores se debe exigir la aceptación y conocimientote la política así como su cumplimiento dentro de las instalaciones o accesos que tengan a AREVALO S.A.

3.8 Aspectos Relevantes De La Política De Seguridad De La Información

- Proteger la privacidad de la información de nuestros clientes.
- Proteger los procesos de creación, procesamiento y resguardo de la información.
- Garantizar que el acceso, intercambio o procesamiento de la información por parte de terceros sea realizada cumpliendo con los más altos estándares de seguridad de la información.
- Asegurarse que la información esté disponible en el momento que los usuarios la requieran.
- Mejorar el costo-eficiencia de los controles de seguridad y su contribución a la rentabilidad del negocio.
- Sensibilizar a los usuarios para garantizar el cumplimiento de las políticas de seguridad.

3.9 Administración De La Política De SGSI

El documento original en medio electrónico reposa en la siguiente dirección electrónica: http://AREVALOSA.COM/INTRANET/

El documento original en medio físico reposa en la oficina de la Gerencia General.

Mantienen copia física controlada de este documento los cargos relacionados en la lista de distribución.

Quienes se relacionan como poseedores de una copia controlada de este manual en la lista de distribución son informados de sus modificaciones y oficialización vía mail, enviando, y se les orienta sobre la ubicación electrónica del mismo para que pueda ser consultado o impreso en el momento en que se requiera.

El líder del proceso de seguridad de la información, es responsable por la administración de este documento, garantiza la actualización del documento electrónico en la dirección especificada y de las copias físicas controladas que se relacionan en este manual.

EL Líder del proceso así como los directores de AREVALO S.A pueden suministrar copias controladas de este documento por cualquier medio a entidades externas a la organización, previa la autorización por parte del Líder del proceso de seguridad de la información de AREVALO S.A, de tal modo que dicha copia se registre debidamente en el listado de copias controladas para asegurar su permanente actualización.

3.10 Alineación De Los Objetivos De Seguridad Con Los Objetivos Estratégicos De Negocio

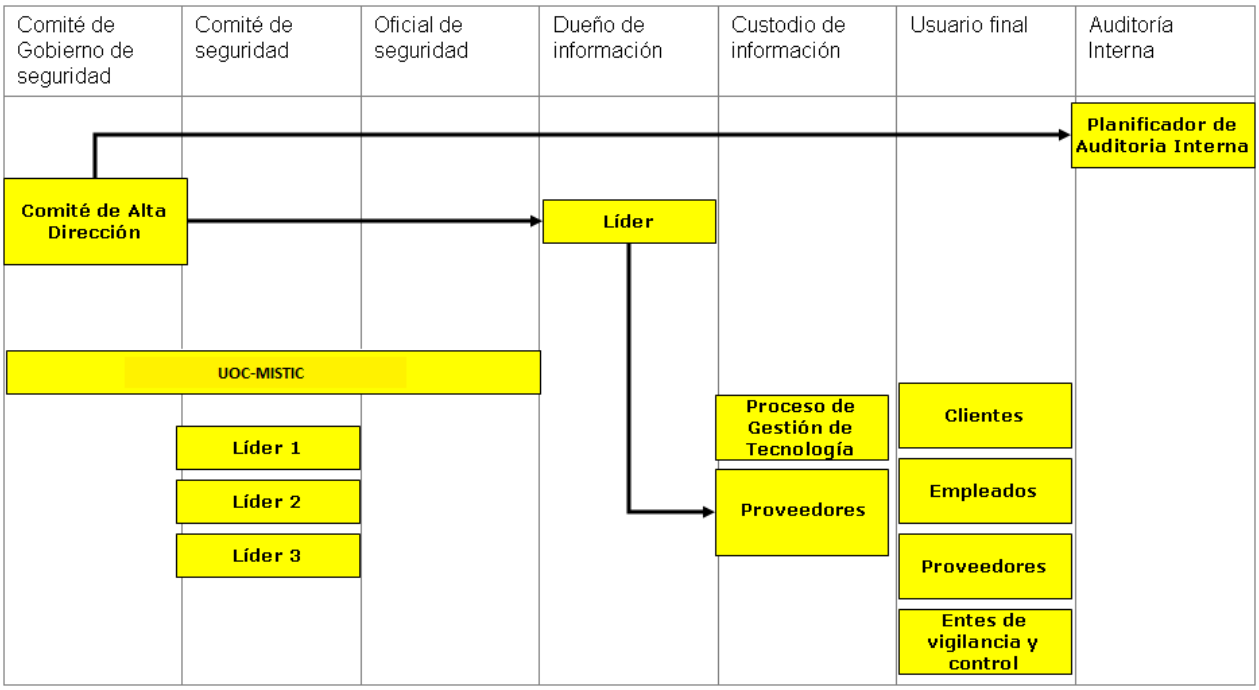
ASPECTO ESTRATÉGICO	OBJETIVOS ESTRATEGICOS	OBJETIVOS DE SEGURIDAD
Mercadeo y Producto	1. Consolidar un portafolio integral de servicios alimenticios de productos de mar.	• Asegurar la satisfacción de los usuarios con altos niveles de protección de su información. • Asegurar el uso y desempeño adecuado de los sistemas que crean, procesan o resguardan información. • Crear agilidad en el procesamiento seguro de la información. • Entregar proyectos de seguridad a tiempo y dentro del presupuesto establecido cumpliendo con los
	2. Fortalecer la internacionalización de los productos alimenticios de mar.	
	3. Consolidar un valioso portafolio de servicios dirigido a las empresas que distribuyan los productos.	
	4. Desarrollar programas que mejoren la producción de los productos alimenticios.	

ASPECTO ESTRATÉGICO	OBJETIVOS ESTRATEGICOS	OBJETIVOS DE SEGURIDAD
	5. Desarrollar el modelo de responsabilidad social empresarial de AREVALO S.A y promover la responsabilidad social empresarial en la región.	estándares de calidad. • Asegurarse que los procesos de negocio protejan la información de manera rentable, mejora continua y esta lista para cambios futuros.
	6. Promover el desarrollo empresarial de la región	
	7. Promover la cultura de conservación del medio ambiente en la región.	
	8. Posicionar a AREVALO S.A como una empresa de alto impacto social.	
	9. Desarrollar nuevos productos.	
	10. Optimizar la prestación de los servicios.	
Diferenciación (Operación)	11. Desarrollar y potencializar la infraestructura física, logística y tecnológica AREVALO S.A.	• Establecer controles de seguridad en los procesos de negocio automatizado, efectivo y eficiente. • Adquirir y mantener sistemas de seguridad integrados y estandarizados. • Integrar controles de seguridad aplicables y tecnológicos en procesos de negocio. • Asegurar la satisfacción de los usuarios con altos niveles de protección de su información. • Asegurarse que la información de los procesos esté disponible en el momento que se requieran. • Entregar proyectos de seguridad a tiempo y dentro del presupuesto establecido cumpliendo con los estándares de calidad. • Asegurarse que los procesos de negocio protejan la información de manera rentable, mejora continua y esta lista para cambios futuros. • Responder con los requerimientos de gobernabilidad alineados con dirección de la Junta Directiva. • Establecer claridad del impacto del negocio en las fallas de seguridad de
	13. Desarrollar alianzas estratégicas con organismos públicos y privados del orden regional, nacional e internacional.	
	17. Garantizar la estabilidad económica de AREVALO S.A.	
	18. Garantizar la consecución de recursos financieros a partir de alianzas y de Cooperación internacional.	

ASPECTO ESTRATÉGICO	OBJETIVOS ESTRATEGICOS	OBJETIVOS DE SEGURIDAD
		la información.
Desarrollo de Colaboradores	14. Fomentar la cultura de trabajo en equipo. 15. Propiciar un clima organizacional favorable.	• Establecer y gestionar una estrategia de sensibilización para aumentar las competencias de seguridad que respondan a la estrategia de seguridad de la información.
Gestión	12. Desarrollar el sistema de gestión de AREVALO S.A articulado al Sistema de Gestión de la Calidad. 16. Desarrollar el modelo de gestión del talento humano.	• Adquirir y mantener una infraestructura de seguridad integrada y estandarizada. • Asegurar la información proveída en las relaciones con terceros. • Mejorar el costo-eficiencia de los controles de seguridad y su contribución a la rentabilidad del negocio.

3.11 Roles Y Responsabilidades

Para gestionar el modelo de seguridad de la información se establecen los siguientes roles y responsabilidades, presentados en la siguiente ilustración.



3.11.1 Comité de Gobierno de Seguridad

Descripción

El comité de gobierno de seguridad debe asistir a AREVALO S.A en todos los temas relacionados con la definición y alineamiento de la estrategia de seguridad, asignación de roles, responsabilidades y niveles de autoridad, gestión y asignación de recursos, validación y gestión de riesgos y en el apoyo para el cumplimiento de los objetivos de negocio.

Responsabilidades

- Aprobar la estrategia de seguridad de AREVALO S.A, con iniciativas tácticas (plan de seguridad) y proyectos que soporten los objetivos de negocio definidos.
- Aprobar el presupuesto de seguridad de la Información y garantizar que los gastos relacionados con seguridad y los proyectos cumplan de forma continua con los requerimientos de negocio.
- Monitorear la estrategia de seguridad, validando su adecuada implementación y recomendando y/o incluyendo nuevos proyectos de seguridad que apoyen el cumplimiento de los objetivos estratégicos.
- Revisar y aprobar las políticas de seguridad o estándares nuevos o modificados.
- Monitorear y evaluar la ejecución de la organización de la seguridad de la información de acuerdo con los indicadores definidos.
- Revisar y modificar las prioridades de las iniciativas de seguridad.

- Revisar y apoyar el presupuesto anual de la organización de la seguridad de la información.

3.11.2 Comité de Seguridad de la Información

Descripción

El comité de seguridad se enfoca en el seguimiento del cumplimiento de tareas tácticas y operacionales de seguridad de la información.

Responsabilidades

- Definir los recursos de seguridad de la información para soportar los requerimientos tácticos, estratégicos y operacionales en las funciones e iniciativas de seguridad.
- Monitorear los planes y proyectos relacionados con seguridad e iniciativas para la entrega de valor, resultados esperados en el tiempo y presupuesto definido.
- Monitorear y revisar los recursos y prioridades que afecten los proyectos de seguridad de la información.
- Gestionar las métricas de seguridad aprobadas por la alta dirección, monitoreando su cumplimiento y el impacto sobre el estado de la seguridad de la información.
- Aprobar los planes proyectados, realizar seguimiento, estimar presupuestos y establecer prioridades y objetivos.
- Desarrollar las políticas de seguridad basado en las mejores prácticas de la industria, los riesgos de AREVALO S.A y de su entorno, y presentarlos al comité de gobierno para su aprobación.
- Establecer guías, estándares y procedimientos operativos que complementen las políticas de seguridad.

3.11.3 Dueño de la Información

Descripción

Es responsable de la información que le sea asignada, así como de su clasificación, control y monitoreo del uso y gestión.

Responsabilidades

- Mantener actualizado el inventario de activos de información de los procesos a su cargo.
- Determinar el nivel de clasificación de la información de la cual es responsable, de acuerdo con su impacto para el negocio y sus objetivos estratégicos.
- Asegurar el cumplimiento de la política de seguridad de la información para garantizar la confidencialidad, la integridad y la disponibilidad de sus activos de información.
- Identificar los riesgos a los cuáles se encuentran expuestos los activos de información a su cargo.
- Definir los controles necesarios para sus activos de información de acuerdo con los niveles de clasificación establecidos y el nivel de seguridad requerido.
- Validar la operación de los controles definidos.

- Aprobar el acceso de empleados y terceros a su información para garantizar que únicamente se realiza cuando sea necesario.
- Monitorear los niveles de acceso de empleados y terceros a su información para garantizar la confidencialidad e integridad.
- Comunicar las novedades de personal a Recursos Humanos con el fin de que se vean reflejadas en los privilegios de acceso de los usuarios a los recursos de información.

3.11.4 Oficial de Seguridad

Descripción

Es el delegado por el Comité de Gobierno de Seguridad de AREVALO S.A para implementar la estrategia de seguridad de la información alineada con los objetivos del negocio, dirigir el programa de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de las políticas y directrices definidas y aprobadas por AREVALO S.A.

Responsabilidades

- Garantizar el alineamiento estratégico de la seguridad de la información con los objetivos de negocio.
- Desarrollar la estrategia de seguridad de la información de AREVALO S.A.
- Supervisar la implementación de la estrategia de seguridad de la información.
- Asegurar el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento continuo del sistema de gestión de la seguridad de la información.
- Asegurar la actualización periódica de la política de seguridad de la información y las directrices y procedimientos que la soportan.
- Asegurar el debido cumplimiento de la política de seguridad de la información de AREVALO S.A.
- Evaluar y aprobar las iniciativas planteadas en función del fortalecimiento del sistema de gestión de seguridad de la información de AREVALO S.A.
- Dirigir el mantenimiento y actualización periódica del inventario de activos de información.
- Dirigir y monitorear la ejecución de evaluaciones de riesgo e impacto al negocio.
- Asegurar la implementación de estrategias adecuadas de tratamiento de los riesgos identificados para los activos de información.
- Definir métricas que permitan monitorear el desempeño del sistema de gestión de seguridad de la información y su valor otorgado a la organización.
- Asegurar la definición y optimización de los recursos asignados al cumplimiento de la estrategia de seguridad.
- Apoyar al Comité de Gobierno de seguridad en la definición de las competencias y habilidades requeridas para los cargos que deben asumir los roles establecidos como parte del gobierno de seguridad de AREVALO S.A.
- Apoyar a los diferentes dueños de la información en la definición y despliegue del programa de conciencia, entrenamiento y educación en seguridad de información.

- Incluir dentro de los planes de entrenamiento de los empleados de AREVALO S.A lo relacionado con seguridad de la información.
- Apoyar el desarrollo de un esquema de sanciones por incumplimiento de las políticas y directrices de seguridad de la información.
- Apoyar al Comité de gobierno de seguridad en la divulgación de las políticas y directrices de seguridad de la información definidas por AREVALO S.A.

3.11.5 Usuario final

Descripción

El usuario final es cualquier empleado, proveedor, contratista, u otra persona autorizada, que utiliza la información de AREVALO S.A en la ejecución de las actividades de su trabajo diario.

Responsabilidades

- Mantener la confidencialidad de la información sensible proveída por la organización para llevar a cabo sus labores diarias.
- Reportar las violaciones a los lineamientos de seguridad definidos por AREVALO S.A al comité de seguridad.
- Aceptar, comprender y aplicar las políticas, estándares y controles técnicos de seguridad de la información de la organización.
- Utilizar la información y recursos corporativos de forma ética, responsable y confidencial.

3.11.6 Custodio de la información

Descripción

El custodio de la información es cualquier empleado, proveedor, contratista, u otra persona autorizada, que tiene la responsabilidad de mantener y/o de soportar los controles de seguridad en los activos de información que contienen la información corporativa.

Responsabilidades

- Garantizar que se cumplan los niveles de servicio definidos.
- Mantener y soportar los controles de seguridad establecidos en el activo para proteger la información.
- Proporcionar asistencia al Dueño de la Información en la selección de soluciones técnicas apropiadas y controles de protección de la información.
- Proveer operativamente el aseguramiento de la Confidencialidad, Integridad y Disponibilidad de la información.

3.11.7 Auditoría Interna

Descripción

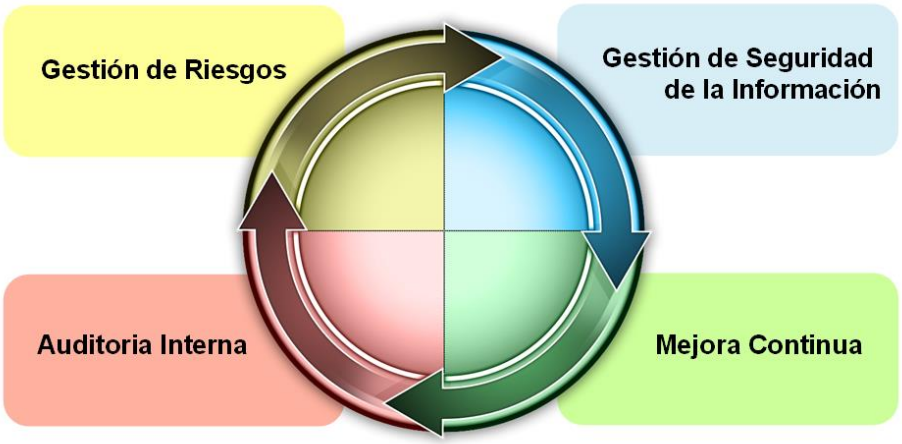
Es encargado de asegurar, de manera independiente, el cumplimiento adecuado de los objetivos establecidos en la estrategia de seguridad de la información de AREVALO S.A proveyendo seguridad razonable sobre la conservación de los niveles de confidencialidad, integridad y disponibilidad requeridos según la naturaleza e impacto de los activos de información.

Responsabilidades

- Definir procedimientos de pruebas independientes que permitan evaluar el diseño y eficacia operativa de los controles establecidos para proteger los activos de información de AREVALO S.A.
- Emitir recomendaciones para el mejoramiento continuo de los controles establecidos para proteger los activos de información de AREVALO S.A.
- Reportar al Comité de Gobierno de Seguridad las brechas encontradas frente a los objetivos establecidos en la estrategia de seguridad de la información.
- Monitorear la implementación de recomendaciones para el cubrimiento de las brechas identificadas y reportadas
- Revisar el cumplimiento de las políticas y directrices de seguridad de la información definidas por AREVALO S.A
- Reportar al Comité de Gobierno de Seguridad los casos de incumplimiento de las políticas y directrices de seguridad de la información.

3.12 Procesos Del SGSI

La siguiente ilustración muestra los procesos que soportan el SGSI de AREVALO S.A.



xxxxx Procedimiento de Gestión de Riesgos: Establece las directrices para la identificación, análisis, monitoreo y tratamiento de los riesgos asociados a los procesos y procedimientos definidos para AREVALO S.A.

Xxxxx Procedimiento de Gestión de Seguridad de la Información: El objetivo es proveer los mecanismos adecuados y suficientes para garantizar la confidencialidad, integridad y disponibilidad de la información de la Organización.

Xxxxx Procedimiento de auditoria interna: Definir los lineamientos que deben tenerse cuenta para la planeación y ejecución de auditorías de seguridad de la información de AREVALO S.A, con el propósito de preservar los principios de seguridad (integridad, confidencialidad y disponibilidad) de la información.

Xxxx Procedimiento de Mejora Continua: Establece los puntos que determinan o identifican mejoras al SGSI de AREVALO S.A.

3.13 Obligaciones del poseedor

Este es un documento de uso interno exclusivamente y la duplicación no autorizada del mismo para uso externo se considera como violación al código de ética de la organización, dando lugar a las sanciones que se dispongan para el efecto.

Los líderes de los procesos son responsables por el adecuado uso que se haga de las copias impresas de este manual. Cuentan, como mínimo, con una copia física de este manual, para que pueda ser consultada por los funcionarios a su cargo. Son responsables por asegurar que las copias impresas correspondan en todo momento con la edición vigente.

Todo funcionario que posee una copia de este manual tiene la obligación de consultar si cuenta con la edición vigente del documento previo a la utilización del mismo y, salvo las funciones autorizadas para ello, no está facultado para duplicar bajo ningún mecanismo el documento.

3.13 Metodología Usada en la Medición del Riesgo

Como metodología empleada en la medición del riesgo se usara **MAGERIT.** A continuación se describen los elementos más importantes de esta metodología de análisis de riesgos.

MAGERIT persigue los siguientes objetivos:

Directos: Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos: Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

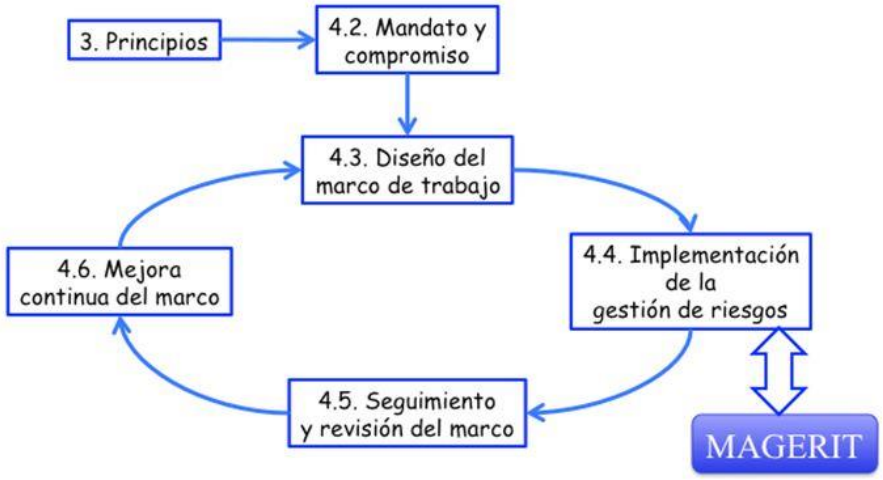


Figura 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Las técnicas a utilizar durante el análisis de gestión de riegos serán las siguientes:

Técnicas específicas para el análisis de riesgos

- análisis mediante tablas
- análisis algorítmico
- árboles de ataque

Técnicas generales

- técnicas gráficas
- sesiones de trabajo: entrevistas, reuniones y presentaciones
- valoración Delphi

Las fases a trabajar son las siguientes:

A continuación se detalla una breve descripción de cómo se abordara el diseño de estas fases:

1. Caracterización del sistema	etapas de la metodología base
2. Identificación de vulnerabilidades	
3. Análisis de controles	

De las etapas anteriores se obtiene la Fase I de la siguiente manera:

Fase I: identificación y evaluación de los elementos críticos de la organización

Esta fase contempla 2 procesos:

1. Identificar, Analizar y Valorar los Activos de la Organización.
2. Analizar la Vulnerabilidad y Determinar la Calidad de los Controles o Servicios de Seguridad

Continuando de igual manera con otras dos etapas de la metodología base, tenemos:

Identificación de amenazas	Etapas de la metodología base
Determinación de la probabilidad de ocurrencia	

De las etapas anteriores se obtiene la Fase II de la siguiente manera:

Fase II: determinación de las amenazas e impactos sobre los activos relacionados

Esta fase contempla 2 procesos:

1. Identificar y Determinar las Amenazas en Relación a los Activos Críticos.
2. Definir la Probabilidad de ocurrencia de una amenaza.

Seguimos con otras dos etapas de la metodología base:

Análisis del impacto	Etapas de la metodología base
Determinación del Riesgo	

De las etapas anteriores se obtiene la Fase III de la siguiente manera:

Fase III: análisis del impacto y del riesgo

Esta fase contempla 2 procesos:

1. Valorizar y Estimar el Impacto sobre los Activos Críticos.
2. Analizar y Estimar el Riesgo

Finalmente tomamos las dos últimas etapas de la metodología base:

Recomendaciones de Control	Etapas de la metodología base
Documentación de resultados	

De las etapas anteriores se obtiene la Fase IV de la siguiente manera:

Fase IV: gestión de riesgos

Esta fase contempla 3 procesos:

1. Interpretación de los Resultados
2. Determinar Medidas de Seguridad
3. Documentación del Proceso de Análisis de los Riesgos

3.14. Procedimiento de Auditorías Internas

3.14.1 Propósito del documento.

Este procedimiento pretende definir los lineamientos que deben tenerse cuenta para la planeación y ejecución de auditorías de seguridad de la información de AREVALO S.A, con el propósito de preservar los principios de seguridad (integridad, confidencialidad y disponibilidad) de la información.

3.14.2 Alcance del documento

Este procedimiento está definido para llevar a cabo la planeación y ejecución de auditorías de seguridad de la información, en donde se encuentran involucrados:

- El Oficial de Seguridad, quien debe definir, gestionar, monitorear y verificar el cumplimiento de las políticas y procedimientos establecidos.

- Áreas Involucradas, grupo de personas encargadas de cumplir normas, políticas y procedimientos de la compañía.

3.14.3 Conceptos Claves

- **Activos**: Elemento que tiene valor para la organización.
- **Disponibilidad**: seguridad de que los usuarios autorizados tiene acceso a la información y a los activos asociados cuando lo requieren.
- **Confidencialidad**: seguridad de que la información no está disponible o divulgada a personas o entidades o procesos no autorizados.
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; adicional mente, otras propiedades pueden también ser involucradas tales como autenticidad, registro, no rechazo y credibilidad.
- **Evento de seguridad de la información**: un caso identificado de un sistema, servicio o estado de la red indicando una posible violación de las políticas de seguridad de la información o falla de control, o una situación desconocida nuevamente que puede ser importante en la seguridad.
- **Incidente seguridad de la información**: uno o una serie de eventos de seguridad de la información no esperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Sistema de gestión de la seguridad de la información SGSI**: parte del sistema de gestión global, basada en un enfoque de los riesgos de un negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Integridad:** protección de la exactitud y estado completo de los activos.

- **Riesgo residual**: nivel restante de riesgo después de que se han tomado medidas de tratamiento de riesgo.
- **Aceptación del riesgo:** decisión de asumir el riesgo.
- **Análisis de riesgo**: uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Valoración del riesgo**: proceso global de análisis y evaluación del riesgo.
- **Evaluación del riesgo**: proceso de comparar el riesgo estimado contra el criterio de riesgo establecido para determinar la importancia del riesgo .
- **Gestión del riesgo**: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Tratamiento de riesgo**: proceso de selección e implementación de medidas para modificar el riesgo.
- **Declaración de aplicabilidad**: documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

3.14.4. Conceptos Claves

Son los usuarios administradores de las actividades para éste procedimiento:

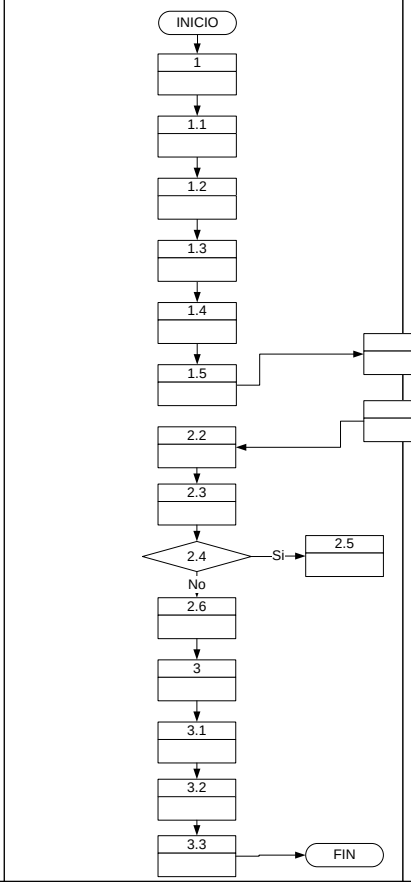
CARGO	FUNCIÓN
Oficial de seguridad de la Información.	Validar los requerimientos solicitados por los jefes o gerentes. Participar en la actualización del procedimiento.
Áreas Involucradas	Cumplir y ejecutar planes de auditoria de seguridad de la información.

3.14.5. Proceso de Planeación y Ejecución de auditorías de Seguridad de la información

El flujo normal de planeación y ejecución de auditorías de seguridad de la información se despliega en el siguiente flujo grama.

PROCEDIMIENTO DE PLANEACION Y EJECUCIÓN DE AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN

No.	Actividades	Oficial de Seguridad /Auditoria Interna	Areas Involucrada
1	Definición de los objetivos de control a Auditar		
1.1	Elaborar plan de Auditorias de Seguridad de la Informacion		
1.2	Definir los recursos necesario para la ejecución de los planes de Auditoria		
1.3	Definir la pruebas a ejecutar en cada plan de auditoria		
1.4	Elaborar un cronograma de Auditoria para la realización de las auditorias		
1.5	Elaborar un Plan de comunicaciones de Auditorias		
2	Ejecutar los planes y cronograma de Auditoria de Seguridad de información		
2.1	Ejecutar las pruebas establecidas en los planes de seguridad		
2.2	Documentar los hallazgos de Seguridad de la informacion.		
2.3	Verificar los incumplimientos de seguridad		
2.4	Cumple?		
2.5	Informar Incidente de Seguridad		
2.6	Elaborar informe de Auditoria		
3.	Desarrollar y monitoreas los planes de acción respecto a los hallazgos de Auditoria		
3.1	Elaborar los planes de accion correcitiva y de mejora.		
3.2	Entregar los planes de acción correctiva y de mejora a las áreas involucradas		
3.3	Monitorear el cumplimientos de los planes de acción correctiva y de mejora en las areas involucradas		



3.15. Política de Seguridad

Control Documental

Versión	Autor	Fecha	Descripción
1.0	UOC-MISTIC	Marzo 28 2013	Versión Inicial

Revisión del Documento

Nombre	Cargo	Versión	Fecha	Comentarios
Gustavo Arévalo Arenas	Gerente de Proyecto	1.0	Marzo 28 2013	Ninguno

Aprobación del Documento

Versión	Aprobación	Fecha	Descripción
Gustavo Arévalo Arenas	Gerente de Proyecto	Marzo 28 2013	Ninguno

3.15.1. Introducción

La información relacionada con los procesos de negocio de AREVALO S.A, es un activo de mucho valor para la organización, por lo tanto requiere una protección del uso no adecuado, de su publicación no autorizada, de robo, alteración o destrucción. Una gestión de seguridad de la información efectiva garantiza que pueda ser compartida mientras se minimiza su exposición al riesgo.

Amenazas que pueden afectar la seguridad de la información se incluyen, pero no se limitan a:

- Error.
- Fraude.
- Código malicioso.
- Desastres naturales.
- Terrorismo.
- Espionaje.
- Interrupción del Servicio.
- Hackers.
- Sabotaje

Esta Política de Seguridad de la Información del SGSI se ha desarrollado para garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos (ej.: sistemas de información, aplicaciones, instalaciones, etc.) de los procesos de negocio de AREVALO S.A, y está alineada con el estándar de industria ISO 27001 “Requerimientos – Sistema de Gestión de Seguridad de la Información – Técnicas de seguridad – Tecnologías de Información”. Al implementar esta política todas las personas involucradas, tanto empleados como proveedores, deben garantizar la protección de los procesos, la reputación y la mejora continua.

3.15.2. Alcance

La política de Seguridad de la Información del SGSI aplica a todos los activos de información, equipos de proveedores y terceros que crean, procesan o resguardan la información de los procesos de negocio de AREVALO S.A.
Está dirigida a funcionarios, proveedores, contratistas, consultores y demás terceros que utilicen información dentro de los procesos de negocio.

La garantía del cumplimiento de esta política debe ser responsabilidad de todos y cada uno de los que intervienen en los procesos y su cumplimiento será auditado por los entes de control interno de la AREVALO S.A.

3.15.3. Audiencia

La presente política debe ser publicada con el fin de que sea conocida, aceptada y cumplida por los empleados, proveedores y clientes que crean, procesan o resguardan la información de AREVALO S.A. Esta política aplica a:

- Todos los empleados que soportan las actividades de gestión y soporte de los procesos de negocio.
- Todos los proveedores y socios estratégicos que aportan en la gestión de operaciones de los procesos de negocio.
- La relación con compañías u organizaciones externas que comparten información con AREVALO S.A.
- Toda la tecnología y actividades de procesamiento de información de los procesos de negocio.

3.15.4. Sistema de Gestión de Seguridad de la Información

Un sistema de gestión de seguridad de la información (SGSI), es un marco que define la metodología con la cual AREVALO S.A protege los activos de sus procesos de negocio y garantiza que las medidas de seguridad apropiadas son implementadas. Es responsabilidad del Proceso de Seguridad de la Información la creación y documentación de un SGSI y de los controles asociados.

El SGSI debe ser desarrollado adoptando el modelo PHVA (Planear, Hacer, Verificar y Actuar). Los componentes básicos de dicho modelo se resumen a continuación:

Planear	Establecer el SGSI con la creación de políticas, estándares, procedimientos, estructura organizacional y procesos de seguridad relacionados con infraestructura tecnológica y no tecnológica; con el fin de identificar, analizar y tratar el riesgo, para garantizar el cumplimiento de la seguridad y los objetivos de negocio de AREVALO S.A.
Hacer	Implementar, operar y monitorear las políticas creadas para el SGSI.
Verificar	Revisar la efectividad del SGSI.
Actuar	Mantener y mejorar el SGSI basado en los resultados de la fase de Verificación.

3.15.5. Planear: Planear el SGSI

Los requerimientos de objetivos de control y controles definidos en esta política deben ser implementados como la base para el desarrollo del SGSI. Este SGSI debe establecerse para cumplir con los requerimientos y para gestionar el riesgo a niveles aceptables. Los controles definidos en el presente documento deben ser implementados por todos y cada uno de los empleados, proveedores y usuarios si sus actividades o labores lo requieren.

La gestión de los riesgos identificados se debe llevar a cabo utilizando el proceso definido a continuación.

1. La política del SGSI debe incluir, pero no estar limitada a lo siguiente:

    - Un marco de trabajo documentado para definir el alcance, los límites y objetivos para establecer una dirección y principios de acción soportados en la seguridad de la información.
    - Análisis y documentación de los requerimientos de negocio, legales y regulatorios, y obligaciones de seguridad contractuales específicas de los procesos de negocio.
    - Una metodología de análisis de riesgo donde se establezcan los criterios de que riesgos serán evaluados y como se identificarán los niveles de riesgos.

2. Un responsable del proceso debe llevar a cabo el análisis de riesgo del proceso y debe mantenerlo y gestionarlo para toda la información y la infraestructura tecnológica que soporta el proceso. Esta metodología debe incluir:

    - Identificación de los activos de información que se encuentren dentro del alcance del SGSI y las amenazas y vulnerabilidades que los afectan.
    - Identificación y valoración del impacto potencial y consecuencias en términos de pérdida de integridad, confidencialidad y disponibilidad de los activos si estos son comprometidos.
    - Una metodología para el análisis de la probabilidad de la realización de los riegos de seguridad basado en los controles actuales.
    - Establecimiento de un criterio para determinar los niveles de riesgo aceptable.
    - Habilidad para reproducir resultados consistentes.

3. Utilizando los objetivos de control y los controles de este documento, el SGSI debe ser capaz de identificar y evaluar los métodos y opciones para el tratamiento del riesgo. Estas opciones incluyen:

    - Aplicar controles que cumplan los objetivos de control y que mitiguen y traten apropiadamente el riesgo.
    - Identificar y entender los riesgos basado en los criterios definidos de análisis de riesgo en el establecimiento del SGSI.
    - Evitar actividades que crean riesgos no aceptables.
    - Transferir riesgos a terceros como aseguradoras.

- Obtener una aprobación de la alta dirección de los riesgos residuales.

4. El uso del SGSI debe ser aprobado y autorizado por la alta dirección. La documentación del SGSI creado durante el proceso de aprobación debe incluir una declaración de aplicabilidad (SoA, por sus siglas en ingles), el cual detalla todos los controles requeridos para cumplir con los objetivos de control y las razones de su implementación o exclusión. El SoA debe incluir:

    - Los objetivos de control y controles que están o serán implementados, basado en los controles definidos en este documento y las razones de su selección.
    - Una lista de objetivos de control y controles adicionales basados en los requerimientos regulatorios o de negocio.

3.15.6. Hacer: Implementar el Plan del SGSI

Cuando el SGSI ha sido desarrollado y aprobado por la alta dirección, es vital que sea implementado apropiadamente. Para alcanzar dicho objetivo se debe:

1. Formular un plan de tratamiento de riesgo basado en los objetivos de control que identifican las acciones apropiadas, recursos, responsabilidades y prioridades necesarias para gestionar los riesgos de seguridad identificados por el SGSI.
2. Implementar el plan de tratamiento de riesgo con el fin de cumplir con los objetivos de control identificados en esta política o cualquier objetivo de control identificado durante el proceso de implementación del SGSI.
3. Asignar apropiadamente los roles y responsabilidades y proveer los recursos y presupuesto necesario para implementar los controles para cumplir con los objetivos de control del SGSI.
4. Definir un proceso para medir la efectividad de los controles implementados. Este proceso debe ser capaz de producir resultados consistentes.
5. Implementar programas de sensibilización y entrenamiento de seguridad adecuados para garantizar que todos los empleados comprendan sus responsabilidades y tengan el conocimiento necesario para cumplir con los objetivos de control.
6. Documentar e implementar los roles, responsabilidades y procedimientos necesarios para la implementación de controles que garanticen el cumplimiento de los objetivos de control y garantizar que se pueda proveer una detección rápida de los eventos relacionados con la seguridad.
7. Ejecutar una gestión y operación continua del SGSI.

3.15.7. Verificar: Monitorear y revisar el SGSI

El SGSI debe permanecer bajo un monitoreo y revisión constante para garantizar su efectividad en el cumplimiento de los objetivos de control definidos en la planeación del SGSI.

1. Ejecutar monitoreo y revisión de los procesos, procedimientos y otros controles para:

    - Identificar rápidamente cualquier intento o éxito de falencia en seguridad.

- Proveer a la alta dirección la capacidad de determinar si las responsabilidades de seguridad delegadas al personal o implementadas a través de tecnologías son efectivas para cumplir con los objetivos de control.
- Determinar si las acciones llevadas a cabo cuando ocurren eventos de seguridad o incumplimientos son efectivas.

2. Actualizar de forma regular el análisis de riesgo para confirmar la validez y el conocimiento de resultados anteriores teniendo en cuenta cambios en los objetivos de negocio, procesos y tecnología.
3. Se debe revisar el SGSI regularmente para validar continuamente si cumple con los objetivos de control, mediante un proceso de cumplimiento de certificación, para identificar áreas potenciales de mejora.
4. El Comité de seguridad de la información debe llevar a cabo auditorías periódicas de la implementación y gestión del SGSI.
5. La gerencia debe revisar el resultado del análisis de riesgo y de otras valoraciones de riesgo como auditorías, proceso de cumplimiento de certificación, adicionalmente a los cambios en ambientes operacionales y otras métricas disponibles que soporten e identifiquen modificaciones del SGSI como cambios en el proceso de análisis de riesgo, planes de tratamiento de riesgo y controles de seguridad.

3.15.8. Actuar: Mantener y Mejorar el SGSI

Para que el SGSI sea efectivo debe someterse a cambios continuos para garantizar que sea actual y que cumpla con los objetivos de control respectivos a los procesos de negocio. Se deben establecer procesos para:

1. Implementar las mejoras, cambios y ajustes al SGSI identificados en la fase de monitoreo y revisión.
2. Modificar las políticas, procedimientos, objetivos de control y documentación basados en las mejoras implementadas.
3. Llevar a cabo las acciones preventivas y correctivas necesarias para eliminar los problemas identificados en el SGSI.
4. Garantizar que las mejoras implementadas cumplan con los objetivos de control.

3.15.9. Requerimientos de documentación

La documentación usada por el SGSI debe ser creada y mantenida apropiadamente.

1. Los documentos deben ser aprobados por la alta dirección para validar su suficiencia y aceptabilidad antes de su implementación.
2. Los documentos deben ser revisados periódicamente, actualizados y reaprobados.
3. Un conjunto de procedimientos y procesos adecuados deben ser implementados para garantizar que los documentos y registros sean protegidos y controlados.
4. Cuando un incidente de seguridad ocurra es importante que se trate en el tiempo y con la prioridad necesaria basada en su severidad. En la mayoría de los casos se requiere evidencia para tratar el incidente de forma apropiada: donde y cuando ocurrió, cuáles fueron las circunstancias, la causa, el

resultado y el impacto, etc. Un mantenimiento y obtención apropiada de registros de auditoria puede proveer dicha evidencia.

5. Existen requerimientos legales para la recolección y preservación de la evidencia en el caso de incidentes criminales. No solo es importante mantener los registros, sino proteger y mantener la integridad, disponibilidad y confidencialidad de dichos registros.

3.15.10. Resumen de los requerimientos del SGSI

Se debe retener evidencia que soporte el establecimiento, implementación, operación, revisión y mejora continua del SGSI.

1. La alta dirección debe demostrar el compromiso en el establecimiento, implementación y mejora continua del SGSI.
2. La alta dirección debe presupuestar los recursos y las necesidades de entrenamiento para una implementación efectiva del SGSI.
3. El SGSI debe ser revisado y auditado periódicamente con el fin de analizar la efectividad de acuerdo a los objetivos de control. Estas auditorias deben llevarse a cabo de forma objetiva.
4. El SGSI debe someterse a mejoras continuas soportado en la implementación de recomendaciones, acciones correctivas y preventivas basadas en la revisión y auditorias del SGSI.
5. Se debe desarrollar la siguiente documentación:

    - SGSI, incluyendo alcance y objetivos.
    - Declaración de Aplicabilidad (SoA).
    - Procedimientos mandatarios requeridos por la ISO/IEC 27001 para el control de la documentación y registros, auditorías internas del SGSI, acciones correctivas y preventivas.
    - Otras políticas y procedimientos que soporten el mantenimiento y desarrollo del SGSI.
    - La metodología adoptada para análisis de riesgo.
    - Un reporte que presente los resultados del análisis de riesgo llevado a cabo.
    - Un plan de tratamiento de riesgo que identifique las acciones a realizar para gestionar los riesgos identificados.
    - Procedimientos operacionales que garanticen la implementación efectiva de los controles de seguridad y que demuestre como se mide la efectividad de los controles.
    - Registros que provean la evidencia de la implementación de controles.

3.15.11. Política de Seguridad

Objetivos de Control:

- La información y los activos de AREVALO S.A serán protegidos de amenazas que puedan afectar la confidencialidad, integridad o disponibilidad de los procesos de negocio.
- Es necesario que todas las obligaciones legales, regulatorias y contractuales se cumplan.

- El acceso a la información solo será garantizada si las necesidades de negocio lo requieren.
- Todos los usuarios de los sistemas y de los activos de información serán identificados, responsabilizados y monitoreados en el uso de dichos activos.

Controles:

3.15.12. Documento de la política de la seguridad de la información

Se debe desarrollar un plan de sensibilización para cualquier nueva práctica de seguridad de la información. El plan de comunicación debe incluir, sin limitar, notificación de nuevas prácticas, integración con la estrategia de sensibilización y, en caso de necesidad, entrenamiento especial para usuarios o personal técnico.

La alta gerencia de AREVALO S.A debe aprobar las políticas de seguridad de la información.

Todas las prácticas y estándares de seguridad deben ser revisados y aprobados por el comité de seguridad de la información.

El Comité de seguridad es el responsable de la revisión y de coordinar la aprobación y la puesta en práctica de cualesquier práctica o estándar de seguridad.

3.15.13. Revisión de la política de seguridad de la información

El Comité de seguridad es el responsable de revisar constantemente la implementación y cumplimiento de las políticas de la seguridad de la información de AREVALO S.A.

Un informe anual de revisión debe ser presentado por el Comité de seguridad e incluir como mínimo un análisis de la aplicabilidad en la práctica de la seguridad a los requisitos actuales de tecnología, negocio y procesos.

Los estándares de seguridad serán revisados por el Comité de seguridad, quien es el responsable de realizar una revisión técnica y asegurar que los estándares se actualicen de acuerdo a las necesidades del negocio y prácticas recomendadas.

3.16. Declaración de la Política de Seguridad de la Información.

La información y los activos que generan, procesan o resguardan los datos de los procesos de negocio de AREVALO S.A son de un alto valor para la organización y deben ser protegidos adecuadamente. Los procesos son operados en un ambiente soportado en infraestructura tecnológica que requiere un marco de trabajo estandarizado y consistente el cual garantice la seguridad de la información que procesa.

Para garantizar una protección y mejora continua, la alta dirección de AREVALO S.A cree firmemente en la alineación de la seguridad de la información con los estándares apropiados de la industria.

Es política de AREVALO S.A que los activos de información se protejan de todo tipo de amenazas tanto internas como externas, deliberadas o accidentales, y garantizar que se cumpla con los siguientes requisitos:

- La información de nuestros clientes debe ser protegida.
- La integridad de la información creada, procesada o resguardada por los procesos de negocio debe ser mantenida.
- La confidencialidad de la información debe ser garantizada.
- Los procesos de negocio deben estar disponibles de acuerdo a las necesidades del negocio.
- Todas las obligaciones legales, regulatorias y contractuales deben cumplirse.

El acceso a los activos de información solo debe ser proveído de acuerdo con las necesidades de negocio, y los usuarios individuales de dichos activos deben ser identificados, responsabilizados y monitoreados de acuerdo al uso que le den a sus activos.

Serán desarrolladas políticas de seguridad específicas por temas, abarcando las mejores prácticas mundiales de seguridad de la información.

Las políticas de seguridad de la información se convierten en parte esencial del programa de seguridad de la información, teniendo como objetivo asegurar la plataforma y las actividades que soportan los procesos de negocio de AREVALO S.A.

Todas las personas, empleados y terceros, deben implementar y cumplir con los controles de seguridad definidos en las políticas de seguridad.

Se firma el día 28 de Marzo de 2013

Camila Arévalo Gaviria
Gerencia General
AREVALO S.A.

3.17. Gestión de Indicadores.

3.17.1. Introducción

La información relacionada con los procesos de negocio de AREVALO S.A, es un activo de mucho valor para la organización, por lo tanto requiere una protección del uso no adecuado, de su publicación no autorizada, de robo, alteración o destrucción. Una gestión de seguridad de la información efectiva garantiza que pueda ser compartida mientras se minimiza su exposición al riesgo.

Como todo sistema de gestión se hace necesario que este sea medible, por lo tanto es necesaria la definición de Métricas de seguridad los cuales estas deben cumplir con los siguientes requisitos:

- Debe ser relevante para la organización.
- De ser reproducible y justificable.
- Debe ser objetiva e imparcial.
- Debe ser capaz de medir la evolución de la seguridad en la compañía a lo largo del tiempo.

3.17.1. Definición de Indicadores

A continuación se definen para la Empresa de AREVALO S.A, los siguientes indicadores que se debe ir implantando a lo largo del desarrollo del SGSI para la empresa.

1. Inventarios de Activos Realizados en el año: Se definirá un número específico de inventarios que se debe realizar a los activos de la empresa y su medición se realizar de manera semestral, midiendo los inventarios programados versus los realizados.
2. Escaneo de Vulnerabilidades de seguridad a Activos de procesamiento de información (Servidores): Se definirá un número específico de escaneos de vulnerabilidades que se debe realizar a los servidores de la empresa y su medición se realizar de manera mensual, midiendo los escaneos programados versus los realizados.
3. Aplicación de Controles productos de escaneo de vulnerabilidades de seguridad a Activos de procesamiento de información (Servidores): Teniendo en cuenta los resultados de los escaneos se evaluara la atención y aplicación de controles a las vulnerabilidades encontradas, la medición se realizar de manera mensual, midiendo el número de vulnerabilidades encontradas versus las vulnerabilidades atendidas.
4. Incidentes de Seguridad: Existen diversas formas de reportar incidentes de seguridad de la información, por los empleados de AREVALO S.A, la medición se realizar de manera mensual, midiendo el número de incidentes reportados y se llevaran dos estadísticas, la primera busca medir mes a mes la cantidad de incidentes presentados para marcar una tendencia, y la segunda busca medir incidentes reportados versus incidentes atendidos.
5. Plan de Continuidad: En el momento de que se implemente un BCP en la compañía AREVALO S.A, se implementara un indicador donde se establezcan un número determinado de pruebas al plan y la medición se realizara de manera semestral, midiendo el número de pruebas programadas versus pruebas realizadas durante el semestre.

6. Mantenimientos Preventivos: Se definirán cronogramas de los siguientes Mantenimientos de tipo preventivos:
    - Mantenimientos preventivos de Plataforma de Networking.
    - Mantenimientos preventivos Servidores.
    - Mantenimientos Preventivos Centros de Cableado.
    - Mantenimientos Preventivos Comunicaciones.
    - Aplicación y Revisión de Estándares de Seguridad, en el cual se revise periódicamente que los estándares definidos de seguridad se estén aplicando.
    - Mantenimiento Preventivo Equipos de Cómputo.
    - Mantenimiento Preventivo Software de Control de Código malicioso y virus.

Su medición se basara en la programación en cronograma versus el cumplimiento en ejecución.

1. GLOSARIO

- **Activos**: Cualquier cosa que tiene valor para la organización.
- **Disponibilidad**: seguridad de que los usuarios autorizados tiene acceso a la información y a los activos asociados cuando lo requieren.
- **Confidencialidad**: seguridad de que la información no esta disponible o divulgada a personas o entidades o procesos no autorizados.
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; adicional mente, otras propiedades pueden también ser involucradas tales como autenticidad, registro, no rechazo y credibilidad.
- **Evento de seguridad de la información**: un caso identificado de un sistema, servicio o estado de la red indicando una posible violación de las políticas de seguridad de la información o falla de control, o una situación desconocida nuevamente que puede ser importante en la seguridad.
- **Incidente seguridad de la información**: uno o una serie de eventos de seguridad de la información no esperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Sistema de gestión de la seguridad de la información SGSI**: parte del sistema de gestión global, basada en un enfoque de los riesgos de un negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Integridad:** protección de la exactitud y estado completo de los activos.
- **Riesgo residual**: nivel restante de riesgo después de que se han tomado medidas de tratamiento de riesgo.
- **Aceptación del riesgo:** decisión de asumir el riesgo.
- **Análisis de riesgo**: uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Valoración del riesgo**: proceso global de análisis y evaluación del riesgo.
- **Evaluación del riesgo**: proceso de comparar el riesgo estimado contra el criterio de riesgo establecido para determinar la importancia del riesgo .
- **Gestión del riesgo**: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Tratamiento de riesgo**: proceso de selección e implementación de medidas para modificar el riesgo.
- **Declaración de aplicabilidad**: documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.