POLITICA

SEGURIDAD DE LA INFORMACIÓN

1. IDENTIFICACIÓN

Versión	1.1
Código	PL-PA-AFSI-001
Entrada en Vigencia	02 de octubre de 2015
Publicación	02 de octubre de 2015

Elaborado por Cargo	Jorge Zambrana G. Subgerente de Sistemas

Aprobado por		
Nombre Cargo	**Victor Vidal V.** **Gerente Administración y Finanzas**	
Nombre Cargo	**Gerardo Yoppi LI.** **Jefe Área Diseño de Procesos**	

2. OBJETIVO

Generar la línea base respecto al conjunto de políticas, procedimientos y estándares de seguridad que regulan y sostienen, toda la información del Grupo Saesa, custodiada por la Subgerencia de Sistemas para resguardar la disponibilidad, integridad y confidencialidad de ella.

3. ALCANCE

Este documento es de aplicación para todos los trabajadores de la compañía, obligatoria e independientemente del cargo que estos tengan, ya sea personal de la compañía o personal de empresas contratistas, por servicios transitorios o permanentes y alumnos en práctica del Grupo Saesa.

4. GLOSARIO

Información: es la interpretación que se da a los datos. Por lo tanto, la información es un activo que el Grupo Saesa debe proteger de la divulgación a terceros, modificación no autorizada o destrucción, sea ésta accidental o intencional.

Confidencialidad: es el concepto por el cual se asegura que la información es accedida sólo por las personas autorizadas para ello.

Integridad: es el concepto por el cual se salvaguarda la exactitud y totalidad de la información, tanto en su procesamiento, transmisión y/o almacenamiento.

Disponibilidad: es el concepto por el cual se asegura que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando éstos sean requeridos.

5. Política

Desde la perspectiva de negocio del Grupo Saesa y como parte de los objetivos estratégicos, la información debe ser tratada y protegida como un activo de la compañía, definiendo como política general, el alinearse al estándar internacional ISO 27001, que permite abarcar aspectos del gobierno y seguridad de las TI.

5.1. De la Seguridad de la Información

Consiste en brindar protección frente a algún incidente o hecho de pérdida de información durante su uso, procesamiento y/o almacenaje de la misma, formalizando de esta manera documentos de aplicación, procedimientos operacionales y responsabilidades en los siguientes procesos:

- Procedimientos de operación documentados.
- Definir metodologías y procesos relacionados a la seguridad de la información.
- Mantener la política y estándares de seguridad de información de la organización.
- Comunicar y concientizar aspectos básicos de seguridad de información a los empleados de Saesa
- Evaluar aspectos de seguridad de productos de tecnología y/o sistemas que se utilicen al interior de Saesa.
- Controlar aspectos de seguridad en el intercambio de Información con entidades externas.
- Controles de cambio.
- Procedimiento de gestión de incidentes.
- Separación de los ambientes de:
  - Desarrollo
  - Producción
- Planeamiento y aceptación de sistemas.
- Planificación del *sizing* o capacidad.
- Protección contra software malicioso.
- Respaldo de información y su respectivo almacenamiento.
- Gestión y control de la red.
- Control y administración de acceso a usuarios.

- Tratamiento de sistemas críticos.
- Disponibilidad, respaldo y recuperación de datos,
- Uso eficiente y controlado de herramientas tecnológicas como, internet, correo electrónico.
- Planes que aseguren la continuidad del negocio.
- Actualizaciones de versiones, parches, hotfix, y services pack de seguridad,
- Administración de antivirus y sus revisiones periódicas.

5.2. Gobierno TI

Los servicios TI deben ser administrados buscando eficiencia en conformidad a los recursos económicos y lineamientos estratégicos que el Grupo Saesa disponga para estos efectos.

- Los servicios y funciones de TI deben ser proporcionados con el máximo valor posible (mejor costo/beneficio).
- Los riesgos relacionados con TI deben ser identificados y tratados para que la información se mantenga segura.
- Los planes de TI deben elaborarse alineados a la estrategia del negocio del Grupo Saesa.
- Orientar a la compañía en cuanto a innovación tecnológica aportando así un valor agregado a los servicios que esta aporte a la organización.

5.3. Propietario de la Información

Son Gerentes, Subgerentes y Jefes de Área, donde se genera la información que se utiliza en las operaciones de su unidad. Estos deben ser conscientes de los riesgos relacionados, de tal forma que sea posible tomar decisiones oportunas para su disminución.

5.4. Clasificación de la Información

El Grupo Saesa consciente que la información tiene diferentes grados de sensibilidad e importancia y que algunos elementos pueden requerir un grado adicional de protección o manejo especial, utiliza un esquema de clasificación de la información en donde se define el siguiente conjunto de directrices para establecer los niveles de resguardo de la misma:

- La Subgerencia de Sistemas debe asegurar que la información reciba el nivel de protección de acuerdo al nivel de clasificación de ella.
- La información debe ser clasificada como crítica o no crítica, por las respectivas Gerencias, indicando la necesidad, las prioridades y el grado de protección esperado para su resguardo.
- Por definición del Negocio, declara a las plataformas de los Sistemas SIPRE, SGC, PORTAL y SAP más la Información contenida en ellos como Críticas, debiendo la Subgerencia de Sistemas tomar todos los recaudos necesarios en términos de control de acceso, de respaldo, y manejo de la integridad de la información que dichos sistemas manejan.
- La Subgerencia de Sistemas debe proveer las medidas de seguridad necesarias para proporcionar una protección adecuada a los activos de la Organización, así como controlar, generar responsabilidades, normas de uso y clasificación sobre los activos de información.

También, debido a la sensibilidad de la información, contenida en las plataformas disponibles y/o en los equipos de los usuarios, los propietarios de la información deben cumplir con lo siguiente:

- Revisar periódicamente la clasificación de la información con el propósito de verificar que cumpla con los requerimientos del negocio.
- Determinar los requerimientos de respaldo y la periodicidad de estos.
- Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.
- Tomar acciones adecuadas en caso de violación a la seguridad de la información por hechos ajenos a la Subgerencia de Sistemas.

- Respecto a la Propiedad de la información se define que la información derivada de los sistemas críticos y los procesos asociados a estos, pertenece a la Gerencia o Subgerencias definidas a continuación.

- **Sistema Gestión Comercial**

Proceso	Área dueña de la Información
Conectar Servicios Leer Medidores Facturar Repartir Telemedida	Subgerencia Procesos Comerciales
Recaudar Cobranza	Gerencia Administración y Finanzas
Atender Clientes Marketing	Subgerencia de Clientes y Servicios
Regulación	Gerencia de Regulación

- **Sistema Técnico**

Proceso	Área dueña de la Información
Despacho Gestión de Brigadas Proyectos	Gerencia de Operaciones

- **Sistema Portal**

Proceso	Área dueña de la Información
Call Center	Subgerencia de Clientes y Servicios
WF Proyectos ACP Pérdidas	Gerencia de Operaciones
Autoservicio	Gerencia de Personas

- **ERP**

Proceso	Área dueña de la Información
Recursos Financieros	Gerencia Administración y Finanzas
Contabilidad Tributaria Activo Fijo	Subgerente de Contraloría
Muebles e Inmuebles Abastecimiento Servicios Generales	Subgerente de Abastecimiento
Personas	Gerencia de Personas
Proyectos Nuevos Negocios	Gerente Desarrollo de Negocios
Auditoría	Director de Auditoría Interna
Contratos	Subgerente Legal

- **Sistema CIC**

Proceso	Área dueña de la Información
Recepción de Llamadas Clientes Derivación Teleatentendientes	Subgerencia de Clientes y Servicios

5.5. Custodio de la Información

La Subgerencia de Sistemas, es responsable de monitorear el cumplimiento de los procedimientos e instructivos de seguridad elaborados en base a esta política, para todos los sistemas que administra, como:

- Accesos a nivel de red (Sistema Operativo).
- Accesos a nivel de bases de datos.
- Acceso a medios de almacenamiento físico.
- Implementación de controles definidos para los sistemas de Información, como: investigación e implementación de actualizaciones de seguridad de los sistemas (Service packs, fixes, etc)
- Investigación de brechas e incidentes de seguridad.
- Entrenamiento y concientización a los usuarios y colaboradores en aspectos de seguridad de la información de nuevas tecnologías o sistemas implantados en Grupo Saesa.

- Asistir y administrar los procedimientos de Backup, recuperación y transporte de medios magnéticos.

5.6. Responsabilidad de Usuarios y Colaboradores

Los usuarios y colaboradores del Grupo Saesa como primer garante de la información, deben velar por el procesamiento seguro de ella, lo cual es una obligación laboral diaria, dentro de las responsabilidades del usuario están:

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- Reportar supuestos incidentes y violaciones a la seguridad de la información.
- Asegurarse de ingresar información adecuada a los sistemas
- Adecuarse a las políticas de seguridad de la Información de Saesa.
- Utilizar la información de Saesa únicamente para los propósitos autorizados.

La empresa se reserva el derecho de tomar medidas disciplinarias para sancionar al personal en caso de existir evidencias de no cumplimiento de las disposiciones de la presente política.

5.7. De la Entrega de Recursos en Desuso

La Subgerencia de Sistemas consistente con la definición medioambiental del Grupo SAESA, da cumplimiento a los protocolos definidos por el área de Medioambiente, (GESTIÓN DE RESIDUOS SÓLIDOS EN OFICINAS), no obstante a lo anterior antes de toda entrega aplica un proceso de formateo o borrado total de la data que los dispositivos o cintas de respaldo podrían contener.

5.8. Control y Auditorías

- **Comité de IT:**

  El Grupo Saesa cuenta con un comité de IT compuesto por: el Gerente General, Gerente de Administración y Finanzas, Gerente de Operaciones, Gerente Legal, Gerente de Planificación Estratégica, Gestión y Riesgo y Subgerente de Sistemas.

Este comité se debe reunir cada 3 meses con los siguientes objetivos:

- Dar seguimiento y evaluar el plan de sistemas de mediano y largo plazo.
- Promover, aprobar, establecer normas, políticas y lineamientos para la administración, crecimiento, estandarización, uso y aprovechamiento de los recursos de IT.
- Establecer los mecanismos de coordinación entre las áreas, con el fin de mejorar el uso y aprovechamiento de bienes y servicios de IT.
- Promover el uso de estándares tecnológicos que faciliten las funciones de las áreas.
- Definir una metodología que permita apoyar el proceso de análisis de los requerimientos de bienes y servicios de IT, para su alineación con los objetivos estratégicos.
- Promover la modernización de la compañía conforme a los avances que surjan en el mercado en materia de IT.

➢ **Auditorías de Sistemas:**

La Subgerencia de Sistemas es auditada, según la periodicidad definida por el plan de auditoría interna aprobado por el Comité de Auditoría, por medio de auditores externos independientes.

6. Cumplimiento

Se debe dar cumplimiento a toda disposición vigente, sea esta normativa o legal, la cual debe ser aplicable al caso y lugar que corresponda, según afecte o impacte en los servicios de TI. Dentro del Marco Normativo se deben atender las necesidades de auditorías, revisiones y controles que el Grupo Saesa requiera.

7. CONTROL DE MODIFICACIONES

Fecha Publicación	Versión	Modificación	Fecha Entrada en Vigencia
16-enero-2014	1.0	Versión Inicial 1.0	16-enero-2014
02-octubre-2015	1.1	Se complementa el capítulo de clasificación de la información. Se agrega el capítulo sobre la entrega de recursos en desuso. Se elimina el capítulo de documentos relacionados.	02-octubre-2015