Contenido

1. INTRODUCCIÓN

Para la Alta Dirección de Espumlandia S.A.S. es importante identificar y proteger un activo valioso y a medida como lo es la información, de esta manera evitar la destrucción, divulgación, utilización y modificación no adecuada y/o no autorizada, con estrategias de alto nivel que permitan el permanente control y la administración efectiva de la información de clientes, empleados y proveedores.

Es por esto que Espumlandia S.A.S. formaliza su compromiso con los procesos de gestión responsable de información, con el objetivo de garantizar a las partes interesadas la confidencialidad, integridad y disponibilidad de la información.

2. IDENTIFICACIÓN DE LA EMPRESA

Razón social	ESPUMLANDIA S.A.S.
Nit	800026934-9
Dirección	CR 68N # 36 39 SUR
Ciudad	Bogotá D.C.
Departamento	Cundinamarca
Teléfonos	5337730 - 5337734
Correo electrónico	espumlandia@hotmail.com
Página web	www.colchonesdreamz.com

3. SEGURIDAD DE LA INFORMACIÓN:

El aseguramiento y preservación de la información son las bases de la seguridad de la información, así como el cumplimiento de las siguientes características.

- **Autenticidad**: Los activos de la información se crean, editan y custodian por usuarios autorizados que permanente validan su contenido.
- **Confidencialidad**. Solo se podrá acceder a la información con usuarios y contraseñas que serán entregados al personal que tenga permiso para esto.
- **Confiabilidad**: El contenido de la información conservada debe ser fiable siempre y cuando conserven la confidencialidad, autenticidad, legalidad e integridad.
- **Disponibilidad**: La información debe encontrarse a disponibilidad únicamente de personal autorizado, dentro de los horarios de tiempo establecidos.
- **Integridad**. El contenido de la información debe permanecer completo, sin alteraciones, garantizando de documentar y/o registrar cada modificación que se realice

- **Legalidad**: La información conservada, cumple con los parámetros legales y normativos.
- **Posibilidad de auditoria**: Se mantiene evidencia de cada actividad y acción que pueda afectar la información.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información es un recurso, que al igual que los activos presenta un valor para la empresa, motivo por el cual debe ser protegida.

La generación, seguimiento, mejora y aplicación de la política de seguridad de la información genera un compromiso de protección hacia la misma, teniendo en cuenta las diversas amenazas que se pueden presentar. A partir de esta política se genera la minimización de riesgos asociados a daño y asegura el cumplimiento de las funciones de la empresa que apoyan un correcto sistema de información.

3.1 Alcance

Esta política aplica para todas las dependencias de Espumlandia S.A.S. , la totalidad de procesos internos y/o externos que sean vinculados a la empresa, así como a todo el personal cualquiera que sea su situación contractual y el nivel de tareas que desempeñe.

3.2 Objetivos:

- Administrar, controlar, proteger y preservar la información de Espumlandia S.A.S. Así como los medios tecnológicos que puedan ser usados en el procesamiento de la misma, frente a las diversas fuentes de amenaza internas o externas, producto de acciones deliberadas o accidentales, asegurando el cumplimiento de las características fundamentales de la seguridad de la información. (Autenticidad, Confidencialidad, Confiabilidad, Disponibilidad, Integridad, Legalidad y Posibilidad de auditoria)

- Definir las Directrices de Espumlandia S.A.S. Para la correcta valoración de los riesgos asociados a la información, identificando el impacto y evaluando diferentes opciones para su tratamiento, con el fin de garantizar la integridad de los sistemas de información.
- Mantener la Política de Seguridad de la Información actualizada, vigente, auditada y operativa, asegurando su permanencia y nivel de eficacia.

3.3 Responsabilidades

La política de seguridad de la información es de aplicación obligatoria para todo el personal de Espumlandia S.A.S., sin importar su situación contractual, dependencia o nivel de las tareas que desempeñe para la empresa.

La Alta Dirección realiza la aprobación de esta política y es responsable de autorizar cualquier actualización y/o modificación que se realice sobre esta; así como de brindar autorización y entrega de accesos al personal que se encargara de manejo, actualización y consulta de la información.

El (la) jefe de producción, actuará como líder del proceso de seguridad de la información, será el encargado de garantizar el correcto uso de la información de la empresa, realizando la correcta aplicación de las medidas de seguridad inherentes a la presente política. Así mismo será el encargado de la recepción y respuesta a solicitudes, peticiones, quejas y reclamos, del titular de la información, ejerciendo de esta forma su derecho a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización. (ver procedimiento para tratamiento de solicitudes bases de datos)

La oficina de Gestión Humana, será responsable de notificar al personal que se vincule contractualmente a la empresa, de las obligaciones en el cumplimiento de la presente política de Seguridad de la Información, así como divulgar y capacitar a todos los empleados en la presente política y las actualizaciones o cambios que se puedan presentar sobre la misma.

4 SEGURIDAD FÍSICA Y DEL ENTORNO

4.1 Acceso

Se debe tener acceso restringido y controlado a cuartos de servidores, así como las normas y controles de registro en SIIGO

4.2 Seguridad de los Equipos

El servidor que contiene la información se debe mantener en un ambiente seguro y protegido con.

- Controles de acceso
- Seguridad Física
- Controles de humedad y temperatura
- Bajo riesgo de inundación
- Sistemas de extinción de conflagraciones
- Sistemas eléctricos regulados
- Respaldos por fuentes de potencia ininterrumpida (UPS)

La información digital debe encontrarse en el servidor aprobado por la persona a cargo del departamento de sistemas, así como SIIGO debe asegurar que los servicios están cubiertos por mantenimiento y soporte adecuados de hardware y software.

Los medios que alojan back up de la información o copias de seguridad deben ser conservados de forma correcta de acuerdo a los estándares que establece la presente política.

4.3 Administración de Comunicaciones y Operaciones

Reporte de investigación de incidentes de Seguridad: Todo el personal de la empresa debe realizar de forma responsable y diligente reportes de posibles violaciones de seguridad a la Alta Dirección.

El comité de seguridad será el encargado de mantener los procesos para la investigación de incidentes actualizados y realizar acompañamiento a la Alta Dirección cuando se considere necesario.

Se debe solicitar a SIIGO la información correspondiente a la seguridad de la información.

Con el fin de contar con protección contra software malicioso y hacking la empresa como mínimo en cada puesto de trabajo protección como software antivirus con capacidad de actualización automática, sin opción de des habilitación por parte de los usuarios.

4.4 Back up de Información o copias de seguridad

Toda información correspondiente a los procesos de la empresa debe ser respaldada por las copias de seguridad que se generaran de forma semanal en un Disco externo, custodiado por el Gerente General, que asegure la confidencialidad e integridad de la información allí almacenada.

Las copias de seguridad de información crítica se deben realizar y registrar de acuerdo a los cronogramas definidos por la Alta Dirección.

4.5 Administración de configuraciones de red

La configuración de Firewall, switches y demás dispositivos de seguridad de red, debe ser documentada y debidamente respaldada por una copia de seguridad.

Todos los equipos que sean utilizados dentro de Espumlandia S.A.S.. Deben ser revisados y aprobados por la persona a cargo del departamento de sistemas. No se

debe realizar ninguna conexión de equipos dentro de la red de la empresa si no cuenta con dicha autorización.

4.6 Intercambio de Información con organizaciones externas

Todas aquellas solicitudes de información por entes externos de control deben contar con previa aprobación del Gerente General, quien dirigirá la entrega de información a los responsables de su custodia.

4.7 Instalación de software

Todas las instalaciones de software que se realicen sobre los sistemas de Espumlandia S.A.S. deben ser previamente aprobados por la persona a cargo del departamento de sistemas de la empresa,

Está prohibido realizar la instalación de cualquier software que viole las leyes de propiedad intelectual y derechos de autor. (ver ley 23 de 1982 y relacionadas). La persona encargada del departamento de sistemas realizara la desinstalación de cualquier software ilegal y registrara el hecho como un incidente de seguridad.

5 CONTROL DE ACCESO

El acceso a las tecnologías de información de la empresa debe ser restringido de acuerdo a los perfiles de usuario, el cual es definido por la Alta Dirección y generados por el departamento de sistemas.

5.1 Control de Claves y nombres de usuario

Los accesos a la información restringida deben ser controlados, por medio de sistemas automatizados de autenticación, La Alta Dirección de Espumlandia S.A.S. , en conjunto con SIIGO, serán los encargados del control de contraseñas y usos de los equipos, dichas contraseñas deben ser almacenadas de forma segura, dichas contraseñas deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

La Alta Dirección tendrán bajo su custodia las claves de los servidores y administradores, asegurando confidencialidad de las mismas y cambiándolas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

Como requisito fundamental para la terminación de relación contractual o laboral del personal de Espumlandia S.A.S. el departamento de sistemas debe certificar la cancelación de cuentas asignadas para el uso de recursos de la empresa.

6 TÉRMINOS Y DEFINICIONES

- **Activo de información:** Datos o información propiedad de la empresa que se almacena en cualquier tipo de medio y que es considerada como sensitiva o critica para el cumplimiento de los objetivos.
- **Administración de Riesgos:** Proceso de identificación, control y eliminación a un costo aceptable de los riesgos de seguridad que podrían afectar la información.
- **Evaluación de Riesgos:** Evaluar las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad que ocurran y su potencial impacto.
- **Incidente de Seguridad Informática:** Evento adverso en un sistema de equipos de cómputo o red, que compromete la confidencialidad, integridad, disponibilidad, legalidad y/o confiabilidad de la información.
- **Información:** Toda forma de conocimiento objetivo con representación física, lógica o explicita.
- **Propietarios de la información:** En contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

- **Responsable de la Seguridad Informática:** Persona a cargo de la seguridad de la información, su función principal es supervisar el cumplimiento de la presente política.
- **Sistemas de información:** Conjunto ordenado de elementos cuyas propiedades se relacionan o interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como naturales.
- **Tecnologías de la información:** Conjunto de hardware y Software operados por una entidad que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

La presente política se aplica a partir del 04 de julio de 2017.