POLITICA DE GESTION INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN

1. ALCANCE

La Política de Gestión Integral de Seguridad de la Información de Detergentes Ltda (en adelante denominada como “Empresa”), establece las directrices y responsabilidades para el cumplimiento de los requerimientos necesarios de seguridad de los activos de información de la Empresa y tiene el propósito de brindar protección ante cualquier acto que atente contra la autenticidad, confidencialidad, integridad y disponibilidad de la información y el buen nombre de la Empresa, incluyendo a los socios, trabajadores y/o colaboradores, proveedores, clientes y comunidades (en adelante denominados como “partes interesadas”), que de una u otra forma participen o se encuentren relacionados con las actividades misionales.

2. OBJETIVOS

a. Establecer, incorporar y fortalecer en la Empresa una cultura de seguridad de la información, que asegure la confianza de las partes interesadas.
b. Establecer directrices que aseguren la autenticidad, confidencialidad, integridad y disponibilidad de la información.
c. Definir roles, responsabilidades y autoridades de la seguridad de la información.
d. Asegurar la ejecución de los procesos y recursos de los activos de información.
e. Identificar, gestionar y monitorear los riesgos asociados a la seguridad de la información en los procesos y procedimientos de la Empresa, por medio de revisiones periódicas.
f. Medir de manera periódica y gestionar los incidentes y/o problemas presentados sobre la seguridad de la información.

3. TÉRMINOS Y DEFINICIONES

Activos de información
Son los recursos que recogen, procesan, almacenan y transmiten información en cualquier medio, incluyendo los electrónicos, físicos y verbales de la Empresa.

Autenticación
Procedimiento de confirmación de la identidad de una persona o sistema autorizado para acceder a un Área y/o Departamento específico, sistema de información y servicio tecnológico.

Cambios
Es la modificación, actualización o eliminación de cualquier elemento que pueda afectar los medios de información de la Empresa.

Cifrado

Proceso mediante el cual a un mensaje y/o archivo se le aplica un algoritmo matemático con lo cual se obtiene un mensaje y/o archivo no legible (cifrado).

Código fuente

Es el conjunto de líneas de texto creadas en un lenguaje de programación, que dirigen las acciones que debe seguir un sistema computacional para ejecutar un programa.

Confidencialidad

Característica de la información de la Empresa, por la cual solo está disponible para personas o sistemas autorizados de manera restringida.

Cortafuego (Firewall)

Es una parte de un sistema o servicio de red, que está diseñada para controlar y bloquear el acceso no autorizado y/o tráfico de red; protegiendo a la intranet de posibles intrusiones provenientes de otras redes.

Credenciales de acceso

Son los datos que permiten autenticar a una parte interesada en un sistema de información y generalmente se componen de nombre de usuario y contraseña.

Disponibilidad

Característica de la información que aplica para documentos y servicios de la Empresa, de modo que estén habilitados para ser consultados y utilizados, de acuerdo con las condiciones de acceso permitidas a la persona o sistema autorizado.

Equipos informáticos

Son los elementos de hardware que permiten almacenar, procesar y transmitir información, tales como: servidores, Firewall, IPS, computador de escritorio, portátil, router, modem, access point, teléfonos inteligentes, tabletas, entre otros.

Eventos de seguridad de la información

Ocurrencia de un suceso identificado sobre un sistema, servicio, componente físico o persona en la Empresa, que evidencia una posible brecha o situación previa y desconocida, que puede ser relevante desde el punto de vista de la seguridad de la información.

Extranet

Es la red privada de la Empresa que se extiende más allá de la red interna y que permite la conexión de las partes interesadas externas.

Firma digital
Reproducción fidedigna y exacta de la firma de identificación de una persona, que permite garantizar la autenticidad e integridad de un documento emitido por dicha persona.

Información sensible y/o crítica
Es Información relevante, aquella que constituye el "Know How / Saber hacer" o conocimiento específico y/o técnico de la Empresa, cuyo uso es estrictamente confidencial, esta información hace referencia: a) formulación de productos, b) información estratégica, c) información legal y estatutaria, d) información financiera y tributaria, e) información misional o core del negocio, técnica y especializada.

Integridad
Característica de la información de la Empresa, conforme a su precisión y completitud; por lo cual solo debe ser modificada por personas o sistemas autorizados.

Incidentes de seguridad
Uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones y amenazan a la seguridad de la información de la Empresa.

Línea Ética
Mecanismo de carácter confidencial, reservado y anónimo, establecido para efectuar denuncias de posibles conductas irregulares o impropias (Fraude, Corrupción/Soborno, Lavado de activos, Conflicto de intereses, Uso indebido de información, Malversación de activos, Incumplimiento) por parte de trabajadores, clientes, proveedores y comunidades vinculadas con la Empresa.

Aplicación informática
Programa y/o servicio que permiten realizar diferentes tareas en un equipo informático.

Riesgo
Efecto de la incertidumbre sobre el cumplimiento de los objetivos de negocio.

Seguridad de la información
Preservación de la autenticidad, confidencialidad, integridad y disponibilidad de la información de la Empresa.

Seguridad informática
Es el proceso de aseguramiento de la infraestructura tecnológica y todo lo relacionado con esta y, especialmente, la información contenida o circulante a través de los equipos informáticos.

Servicios tecnológicos
Son todos los servicios relacionados con las tecnologías de la información tales como servicios de impresión, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, entre otros.

Sistema de gestión de seguridad de la información
Compendio de los procesos y procedimientos de la Empresa, encargados de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

Sistema de Información
Programa o conjunto de programas informáticos que incluyen datos o información, los cuales hacen posible la realización de tareas específicas y apoyan las funciones empresariales.

Token
Es un dispositivo o clave de seguridad de uso personal e intransferible que se utiliza para la autenticación, con el fin de reforzar su seguridad.

Zonas seguras
Son las de acceso restringido, destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren equipos informáticos.

4. POLÍTICA DE GESTIÓN INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN

Conforme a las buenas prácticas y estándares internacionales reconocidos, la Empresa emite esta política como base para la implementación del Sistema Integral de Gestión de Seguridad de la Información, con el fin de generar valor a las partes interesadas y a su compromiso con la protección de la información, considerada como un activo principal para la gestión de sus procesos sistémicos, como parte de una estrategia orientada a la continuidad y disponibilidad del negocio, la gestión integral de riesgos, la toma de decisiones y la consolidación de una cultura de seguridad de la información. Además de garantizar el cumplimiento de procesos, procedimientos, requisitos legales, contractuales y regulatorios.

Las partes interesadas deben acogerse a las directrices contenidas en esta Política de Gestión Integral de Seguridad de la Información y a los documentos relacionados con esta, con el propósito de mantener la autenticidad, confidencialidad, integridad y disponibilidad de la información.

Periódicamente se ejecutarán programas de capacitación y concientización, sobre temas relacionados a la seguridad que se deben mantener en el manejo y gestión de los activos de información, con el propósito de generar cultura sobre la seguridad de la información.

La información interna y externa de la Empresa será clasificada para su protección en los siguientes niveles de acuerdo con su contenido y alineada con la Política de Gestión Documental, donde se determinan los controles para su generación, procesamiento, almacenamiento, intercambio y destrucción:

Clasificación de la información	Conceptualización
Confidencial	Corresponde a información sensible y/o critica la cual se considera como Información relevante, aquella que constituye el "Know How / Saber hacer" o conocimiento específico y/o técnico de la Empresa, cuyo uso es estrictamente confidencial y restringido y cuya divulgación puede generar un efecto material adverso para la Empresa; esta información hace referencia, pero no se limita a: a) formulación de productos y b) información core del negocio. Esta debe estar debidamente protegida, mediante todas las medidas disponibles, razonables y apropiadas, tendientes a evitar pérdidas, degradación, destrucción, así como el acceso, uso, manipulación, modificación o divulgación no autorizada.
De uso interno	Información que debe ser manejada únicamente por las Áreas y/o Departamentos intervinientes en los procesos de la Organización, esta información hace referencia, pero no se limita a: a) información estratégica, b) información legal y estatutaria, c) información financiera y tributaria y d) información misional. Si la divulgación no autorizada genera un efecto adverso para la Empresa, será considerada confidencial.
De uso público	Es aquella información cuya divulgación no genera ningún impacto negativo para la Empresa y/o que un tercero pueda hacer uso indebido de la información de la Empresa.

Los controles establecidos dentro de esta Política de Gestión Integral de Seguridad de la Información estarán sujetos a revisión y monitoreo, en cualquier momento y sin previo aviso.

Cualquier incumplimiento de la presente política, será objeto de clasificación, análisis, documentación y toma de medidas correctivas, conforme con los niveles de clasificación definidos en la norma de incidentes de seguridad, con el fin de mitigar posibles afectaciones contra la seguridad de la información en la Empresa. Las medidas correctivas se establecen por parte de la Alta Dirección y/o Dirección (Gerencia) y pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

Asamblea General de Accionistas o la Junta de Socios o la Junta Directiva de la Empresa, según el caso, aprueba esta Política de Gestión Integral de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Empresa.

Las excepciones a esta política deben ser previamente a su implementación: a) autorizadas por la Alta Dirección y/o Dirección (Gerencia) y b) soportadas con un análisis de riesgos.

En la definición, verificación, cumplimiento y revisión de la política de gestión integral de seguridad de la información junto con su estructura de trabajo, las diferentes instancias de la Empresa tienen los siguientes roles y responsabilidades:

4.1 Alta Dirección (Asamblea General de Accionistas o la Junta de Socios o la Junta Directiva de la Empresa, según el caso)

a. Asegurar la confianza de las partes interesadas en los temas relacionados con la seguridad de la información.
b. Aprobar las directrices establecidas en la Política de Gestión Integral de Seguridad de la Información y las actualizaciones anuales de esta política.
c. Nombrar, empoderar y establecer las responsabilidades de la estructura de la gestión integral de seguridad de la información.
d. Verificar el estado de las acciones establecidas, según revisiones previas del Comité de Seguridad de la Información.
e. Aprobar los cambios a la Política de Gestión Integral de Seguridad de la Información.
f. Supervisar los resultados de las evaluaciones del riesgo, las estrategias de tratamiento y las oportunidades para la mejora continua, concernientes a la seguridad de la información.
g. Revisar a intervalos planificados la continua idoneidad, suficiencia y efectividad de la Política de Gestión Integral de Seguridad de la Información.

4.2 Dirección (Gerencia)

a. Instituir, promover, afianzar y asegurar la implementación de la política de gestión integral de seguridad de la información, su compatibilidad con la estrategia, su gestión de cambio y cultura de seguridad de la información en la Empresa.
b. Alinear los requisitos del sistema de gestión de la seguridad de la información con los procesos sistémicos de la Empresa.
c. Asegurar la disponibilidad de los recursos necesarios para el sistema de gestión de seguridad de la información, mediante su dirección y apoyo como contribución a la efectividad del sistema, el logro de los resultados previstos y el mejoramiento continuo.
d. Otorgar relevancia a las directrices del sistema de gestión integral de seguridad de la información, estableciendo mecanismos eficaces de comunicación interna.
e. Aprobar los indicadores de efectividad del sistema de gestión integral de seguridad de la información, alineado a los indicadores de desempeño de la Empresa.

4.3 Oficial de Seguridad de la Información (Subordinado a la Subgerencia de Control)

a. Asegurar el cumplimiento de las directrices definidas en la Política de Gestión Integral de Seguridad de la Información, generando confianza a las partes interesadas a través de una retroalimentación oportuna y veraz.
b. Implementar, verificar y mantener el sistema de gestión de seguridad de la información.
c. Asegurar los activos de información de la Empresa.
d. Desarrollar, mantener y divulgar la Política de Gestión Integral de Seguridad de la Información con las partes interesadas, estableciendo mecanismos para la comunicación interna y externa.
e. Coordinar la implementación y debida diligencia, de las directrices establecidas en esta política con otros roles de seguridad de la información, líderes de los procesos y procedimientos de las diferentes Áreas y/o Departamentos de la Empresa y demás partes interesadas.
f. Entregar informes de estado y seguimiento de la efectividad de la seguridad de la información y los resultados de las evaluaciones del riesgo, las estrategias de tratamiento y las oportunidades para la mejora continua a la Alta Dirección, en el Comité semestral de Seguridad de la Información.
g. Desarrollar y documentar los procedimientos para gestionar y mantener los controles de seguridad de la información.
h. Establecer un proceso de revisión y monitoreo de vulnerabilidades de seguridad de información y gestionar los planes de remediación.
i. Generar cultura, concientizar y capacitar a las partes interesadas, sobre temas de seguridad de la información y monitorear su efectividad.
j. Intervenir activamente en todos los temas concernientes a la seguridad de la información.
k. Monitorear que los registros de auditoría o “logs de auditoría” sobre los sistemas de información, se ejecuten de manera correcta y cumplan con los períodos de retención establecidos.

4.4 Partes interesadas

a. Mantener absoluta reserva y confidencialidad de la información sensible y/o critica de la Empresa y proteger y salvaguardar toda la información que se encuentre a su cargo, para el desarrollo de sus actividades y/o funciones empresariales.
b. Respetar y cumplir las directrices definidas en la Política de Gestión Integral de Seguridad de la Información.
c. Se debe contar con la debida autorización de la Dirección (Gerencia) previa a la realización de copias de información sensible y/o crítica y confidencial, en cualquier medio de almacenamiento (esta información hace referencia, pero no se limita a: Disco Removible, Memoria USB, DVD, CD, Disquete, Escáner, Fotocopia, cinta magnética), o colocar dicha información en Internet o Extranet o cualquier medio de divulgación.

d. Mantener absoluta reserva sobre las credenciales de accesos de los sistemas de información y/o servicios tecnológicos, los cuales son de uso estrictamente personal e intransferible.
e. Una vez autenticado en el sistema de información, no se debe prestar o que este sea gestionado por otra persona.
f. Bloquear, suspender, hibernar o apagar los equipos informáticos de ser necesario, si este se encuentra desatendido y las partes interesadas son las directas responsables de las actividades que se ejecuten en estos.
g. Actualizar la contraseña de acceso una vez se haga entrega del usuario asignado.
h. Crear contraseñas de acceso que sean fáciles de recordar, pero difíciles de identificar por terceros.
i. Preservar en buenas condiciones y en un ambiente seguro los activos de información entregados por la Empresa, para la ejecución de las actividades y/o funciones encomendadas.
j. Los equipos informáticos, los sistemas de información y los servicios tecnológicos y los demás activos de información asignados a las partes interesadas son de uso exclusivo empresarial, para la ejecución de las actividades y/o funciones encomendadas, las cuales deben ser devueltas una vez termine la relación laboral y/o comercial y/o reasignación.
k. Deben solicitar la autorización a quien corresponda, para la instalación de software, hardware y periféricos en equipos informáticos de la Empresa.
l. Reportar los eventos de seguridad de la información que vayan en contravía de lo establecido en esta política, por intermedio de los canales de denuncia establecidos en la línea ética y de la norma de incidentes de seguridad, según corresponda.
m. Todo visitante durante su ingreso, permanencia y salida de las instalaciones de la Empresa debe estar acompañado de un funcionario responsable del Área y/o Departamento encargado.

4.5. Área y/o Departamento de Tecnología de la Información y Comunicación (en adelante denominada como “TIC”)

a. Mantener absoluta reserva y confidencialidad de la información sensible y/o critica de la Empresa y proteger y salvaguardar toda la información que se encuentre a su cargo, para el desarrollo de sus actividades y/o funciones empresariales.
b. Respetar y cumplir las directrices definidas en la Política de Gestión Integral de Seguridad de la Información.
c. Asegurar la confianza de las partes interesadas en los temas relacionados con seguridad informática.
d. Garantizar la disponibilidad de los sistemas de información y realizar la debida diligencia e implementar controles que propendan y mantengan la confidencialidad de la información.
e. Coordinar con otros roles de seguridad informática y las diferentes Áreas y/o Departamentos de la Empresa, el aseguramiento de los activos informáticos.

f. Robustecer los equipos informáticos mediante la aplicación de la norma de Administración y Aseguramiento de Equipos Informáticos: i)bloqueo de unidades (USB y ópticas “CD – DVD”), ii) instalación y actualizaciones de antivirus, iii) conexiones controladas a servicios de red, iv) administración segura sobre acceso y contenido web, v) actualización de parches de seguridad en los sistemas operativos, y vi) establecimiento de reglas de seguridad en Firewall y Sistemas de detección de intrusos (IDS).
g. Establecer configuraciones de bloqueo automático a los equipos informáticos no superiores a quince (15) minutos.
h. Asegurar el uso eficiente de los recursos, mediante el bloqueo de cuentas de usuario que no hayan sido utilizadas durante sesenta (60) días.
i. Otorgar los accesos (internet, red, correo electrónico, servidores, Skype, acceso remoto, impresiones controladas) previamente autorizados por quien corresponda.
j. Realizar informes del estado y seguimiento de los planes de acción definidos y acordados de la seguridad informática con la que cuenta la Empresa, dirigidos a la Dirección (Gerencia) y al Oficial de Seguridad de la Información.
k. Configurar la conexión segura por medio de Red Privada Virtual “VPN” a los equipos informáticos autorizados, que requieren acceso a la intranet de la Empresa.
l. Ejecutar copias de seguridad o respaldo “backup”, de los sistemas de información y de los parámetros de configuración de los servicios tecnológicos.
m. Desarrollar, documentar y mantener normas, procesos y procedimientos de Seguridad Informática.
n. Evaluar la efectividad de la seguridad informática.
o. Monitorear y gestionar las vulnerabilidades de seguridad informática.
p. Intervenir activamente en todos los temas concernientes a la seguridad informática.
q. Llevar a cabo la administración e interventoría de todos los contratos de tecnología y licencias y mantener bajo custodia las licencias y/o el inventario de estas.
r. Asegurar que existan registros de auditoría o “logs de auditoría” o “logs de eventos” sobre los sistemas de información, que se ejecuten de manera correcta y cumplan con los períodos de retención establecidos, así como la realización del monitoreo y gestión de estos, todo alineado a las normas de Administración y Aseguramiento de Equipos Informáticos y de Incidentes de Seguridad.
s. Propender por la existencia de una plataforma tecnológica, que satisfaga los requerimientos de disponibilidad aceptables para la Empresa.
t. propender porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

5. CONTROL DE ACCESO

La Empresa se encuentra comprometida con la aplicación de buenas prácticas de control de acceso, para lo cual estableció las normas de Control de Acceso Lógico y Físico, las cuales enuncian las directrices de aseguramiento y control de acceso a las partes interesadas a las zonas seguras, a los

a los diferentes sistemas de información, servicios tecnológicos y/o Área y/o Departamento de la Empresa.

Anualmente se deben revisar y actualizar las reglas de seguridad definidas y se deben conservar veinticuatro meses los registros de control de acceso.

5.1 A los sistemas de información y servicios tecnológicos

Las partes interesadas previamente autorizadas con credenciales de acceso por la Empresa deben cumplir con lo establecido en las normas de Contraseñas Seguras y de Control de Acceso Lógico, con el fin de asegurar la autenticidad, confidencialidad, integridad y disponibilidad de la información.

5.1.1 Extranet

Las conexiones a la extranet deben ser autorizadas por la Dirección (Gerencia) y/o por quien este designe y únicamente se debe realizar a través de firewalls, de acuerdo con lo establecido en la norma de Control de Acceso Lógico.

5.1.2 Internet

Las partes interesadas que tengan acceso a internet deben ser autorizadas por la Dirección (Gerencia) y/o por quien este designe, solo al contenido web previamente autorizado y este servicio es de uso exclusivo para el desarrollo de sus actividades y/o funciones dentro de las instalaciones de la Empresa, de acuerdo con lo establecido en la norma de Control de Acceso Lógico

Está prohibido el uso de herramientas como módem, bluetooth, wifi móvil, proxy y cualquier otro elemento de hardware y/o software que permita conexiones remotas y atenten contra la seguridad de los sistemas de información y servicios tecnológicos.

5.1.3 Correo electrónico

Las partes interesadas que tengan acceso a correo electrónico asignado por el Área y/o Departamento “TIC” deben tener un computador asignado por la Empresa, deben respetar el estándar de formato establecido por la Empresa y el acceso a correo electrónico de las partes interesadas diferentes a trabajadores y/o colaboradores deben tener adicionalmente la previa autorización de la Dirección (Gerencia).

Los trabajadores y/o colaboradores que tengan acceso a correo electrónico a través de un dispositivo diferente al computador, debe ser autorizado por la Dirección (Gerencia) y/o por quien este designe.

La salida y entrada de correo externo, debe ser autorizado por la Dirección (Gerencia) y/o por quien este designe.

Está prohibido el uso del correo electrónico asignado por la Empresa que:

a. atente contra la absoluta reserva y confidencialidad de la información sensible y/o critica de la Empresa y/o de las partes interesadas.
b. exprese intenciones u opiniones que expongan el buen nombre y/o imagen reputacional de la Empresa y/o de las partes interesadas.
c. expongan al usuario o a la Empresa y que puedan ser interpretados como difamatorios u ofensivos de alguna forma, además que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico.
d. distribuya o envié advertencias engañosas, virus, cadenas de mensajes, correos no deseados de ningún tipo y/o archivos ejecutables.
e. aparente venir de otra persona o suplante a otra persona.
f. sea usado para fines personales y atente contra las directrices mencionadas en esta política.

El correo electrónico asignado por la Empresa a las partes interesadas está sujeto a monitoreo y revisiones por parte del Área y/o Departamento de la Subgerencia de Control y/o Auditoría, en cualquier momento, sin previo aviso y autorizado por la Dirección (Gerencia).

Dentro de las instalaciones de la Empresa está prohibido el uso y/o acceso a correos electrónicos diferentes al correo electrónico asignados por la Empresa, utilizando equipos tecnológicos de propiedad de la Empresa y la excepción a esto debe ser autorizado por la Dirección (Gerencia) y/o por quien este designe.

5.2 Código fuente de las aplicaciones o sistemas de información

El acceso al código fuente de producción debe estar salvaguardado y protegido por el líder del Área y/o Departamento de TIC y el código de fuente de desarrollo debe encontrarse disponible el acceso únicamente a los trabajadores y/o colaboradores de desarrollo del Área y/o Departamento TIC.

El líder del Área y/o Departamento de TIC es el único responsable para autorizar el acceso al código fuente de producción a los trabajadores y/o colaboradores de las Áreas y/o Departamentos de TIC y Auditoría, así mismo, autorizar el acceso al código fuente de desarrollo para Auditoría.

Todo lo anterior, de acuerdo y en cumplimiento a lo establecido en la norma de desarrollo de software.

5.3 Tokens de seguridad y firma digital

Los trabajadores y/o colaboradores que les sea asignado un token o firma digital por la Empresa, deben cumplir lo especificado en la norma de Administración de tokens y firmas digitales, su uso debe ser personal e intransferible y deben dar aviso inmediato en caso de exposición, robo, pérdida y/o daño, de acuerdo con lo establecido en la norma de incidentes de seguridad.

6. RELACIÓN CON PROVEEDORES DE SERVICIOS TECNOLOGICOS Y DE LICENCIAMIENTO

La Empresa debe formalizar mediante contrato escrito todas las relaciones con proveedores de servicios tecnológicos y de licenciamiento y exigir el estricto cumplimiento de lo establecido en esta política y de la norma de Contratación, Prestación e Interventoría de los Servicios Tecnológicos y de Licenciamiento y asegurar la debida divulgación de esta norma a los proveedores.

7. EQUIPOS INFORMÁTICOS

Todos los equipos informáticos deben ser negociados y adquiridos por la Dirección de ACSCA, de acuerdo con lo establecido por el procedimiento para Compras Generales.

Previamente a la entrega de los equipos informáticos a las partes interesadas, el Área y/o Departamento TIC debe cumplir con las normas de Administración y Aseguramiento de Equipos Informáticos.

Las partes interesadas deben evitar el uso y transporte de los equipos informáticos en lugares o medios que no les ofrezcan las garantías de seguridad física necesarias, para evitar exposición, robo, pérdida y/o daño, la cual se debe reportar de forma inmediata a la Empresa, de acuerdo con lo establecido en la norma de incidentes de seguridad.

8. CONEXIÓN REMOTA

La conexión remota debe estar debidamente autorizada y se debe hacer por medio del servicio establecido por la Empresa, el cual deberá contar con una configuración de conexión y seguridad previamente establecida por el Área y/o Departamento TIC. Los accesos autorizados a las partes interesadas deben ser establecidos por periodos de tiempo no mayor a un año y/o de acuerdo con la necesidad y su uso debe personal e intransferible y únicamente para la realización de actividades y/o funciones empresariales, garantizando la confidencialidad, integridad y disponibilidad de la información.

En ninguna circunstancia se deben establecer conexiones en redes públicas tales como, pero no se limita a: hoteles o cafés internet.

9. GESTIÓN DE CAMBIOS

La Empresa debe asumir la gestión de cambio como pieza clave de evolución; los cambios solicitados por las Áreas y/o Departamentos deben encontrarse debidamente soportados y cumplir con las normas de Gestión de Cambios, teniendo en cuenta que un cambio es la construcción, modificación, actualización o eliminación de cualquier elemento o reglamento que pueda afectar la seguridad de la información.

10. DESARROLLO DE PROGRAMAS INFORMÁTICOS

Los programas informáticos adquiridos por terceros o desarrollados por la Empresa para las operaciones internas, deben estar documentados y contener directrices de seguridad y calidad definidas en las normas de Desarrollo de Software; conforme a los requerimientos establecidos durante el ciclo de vida del desarrollo y para nuevos desarrollos de software. Ninguna aplicación informática debe ser desarrollada con fines fraudulentos.

Toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos, deben estar bajo procedimientos de control de cambios y de versionamiento.

11. COPIA DE RESPALDO

Para la Empresa, es fundamental contar con el respaldo de los activos de información (BackUp) puesto que se pueden llegar a generar requerimientos de restauración en una fecha específica o por eventualidades adversas en las cuales se requiera su recuperación. De acuerdo con esto se tiene implementado una norma de respaldo de información, que garantiza la recuperación de sistemas informáticos, servicios informáticos, configuración de servidores, base de datos, datos e información.

12. ESCRITORIO Y PANTALLA LIMPIA

12.1 Escritorio limpio

Las partes interesadas deben mantener limpios y ordenados sus puestos de trabajo y en el momento en que no se encuentre en su zona de trabajo deberá asegurar los medios de almacenamiento extraíbles, la documentación e información sensible y/o crítica de la Empresa.

12.2 Pantalla limpia

Los equipos informáticos de la Empresa deben mantener como fondo de pantalla o papel tapiz la imagen corporativa autorizada, los iconos de las aplicaciones principales para la ejecución de las funciones diarias y no deben contener archivos y carpetas con información sensible y/o crítica de la Empresa.

13. CIFRADO

De acuerdo con la clasificación de la información y a las normas de Administración y Aseguramiento de equipos informáticos y de Contraseñas Seguras, la información que circula entre sistema de información sensibles y/o críticos, debe estar cifrada o protegida con usuario y contraseña.

Las partes interesadas que transfieran información sensible y/o crítica deben enviar archivos protegidos siempre con contraseña.

14. GESTIÓN DE VULNERABILIDADES

El Oficial de Seguridad de la Información debe realizar el proceso de gestión de vulnerabilidades de acuerdo con la norma de Gestión de Vulnerabilidades y Seguridad Informática y gestionar con el Área y/o Departamento de TIC la remediación efectiva de las vulnerabilidades.

15. COMUNICACIONES

Las partes interesadas deben cumplir la norma de Comunicaciones establecida por la Empresa y debe solicitar autorización a quien corresponda para transmitir cualquier información de la Empresa a través de cualquier medio y hacer declaraciones ante medios de comunicación masiva en nombre de la Empresa.

16. CONTINUIDAD DEL NEGOCIO

La Empresa se encuentra comprometida en proporcionar los recursos necesarios para dar una respuesta efectiva en caso de contingencia o eventos catastróficos, que afecten la continuidad del negocio, de acuerdo con lo establecido en las normas de Plan de Continuidad del Negocio y de Plan de Contingencia.

17. SEGURIDAD DEL RECURSO HUMANO

La Empresa debe asegurar los procesos de selección, contratación, durante la vinculación y desvinculación, durante periodos de ausencia y reasignación del recurso humano aplicando la norma de Seguridad del Recurso Humano.

18. CUMPLIMIENTO

La Empresa debe cumplir con los requerimientos de ley y la legislación vigente, esta información hace referencia, pero no se limita a: a) derechos de autor, b) propiedad intelectual, c) SAGRLAFT y d) Habeas Data.

DETERGENTES, LTDA

DANIEL HAIME G.

Representante Legal