Cardelli M. Tyson J
C.I 23.542.402

Rangel C. Carlos A
C.I 21.003.721

Políticas de la empresa

Política General

La seguridad y confiabilidad de la información es de vital importancia para Trade Solutions Latinoamérica (TSLA). Nuestra empresa brinda soluciones de inteligencia de negocio ajustables a las necesidades de nuestros aliados a través de una plataforma web Traking Tool de acceso restringido.

Para el desarrollo de las actividades de TSLA es primordial la presencia de un sistema de información con sus respectivas tecnologías de seguridad. TSLA garantizará el cumplimiento de los acuerdos de confidencialidad de la información con nuestros clientes y así como la integridad y disponibilidad de la misma.

La empresa se compromete a gestionar de manera sistemática y continua los riesgos de la información, identificando los mismos, estimando su probabilidad de ocurrencia, su impacto y desarrollando planes de contingencia en caso de que sucedan. Por lo tanto Trade Solutions reconoce que sus activos de información son de gran relevancia.

Los auditores de Trade Solutions asumen la responsabilidad de confidencialidad con nuestra empresa de la información referente a cada uno de nuestros clientes (Material Fotográfico, Precios entre otros) lo cual refleja en un compromiso personal de cada uno de ellos con todos nuestros clientes externos. Además la empresa garantiza que la información suministrada por nuestros auditores será única y exclusivamente para el

cliente que la solicita. En caso de violación de la seguridad de la información Trade Solutions actuará de acuerdo a lo establecido en la ley contra delitos informáticos.

Objetivos de Seguridad de la información

- Contar con un sistema de seguridad de la información, con la finalidad de mitigar los riesgos operativos y de tecnología de la información
- Contar con personal capacitado en seguridad de la información el cual se encargará del mantenimiento y mejora continua del sistema de gestión de seguridad de la información
- Garantizar un proceso de formación continua al personal de la compañía en lo referente a la seguridad de la información
- Tener en cuenta los requisitos aplicables de seguridad de la información relacionados con la confidencialidad, integridad, disponibilidad autenticidad además de los resultados de la evaluación y tratamiento de riesgos
- Garantizar un proceso de mejora continua al sistema de seguridad de la información
- Documentar y comunicar la información al personal de la empresa

Política de correo electrónico

1. **Información general**

   El correo electrónico se utiliza casi necesariamente en todas las ramas de la industria y es a menudo el principal método de comunicación y sensibilización dentro de una organización. Al mismo tiempo, el mal uso de correo electrónico puede acarrear muchos riesgos legales, de seguridad y privacidad, por lo tanto es importante que los usuarios comprendan el uso apropiado de las comunicaciones mediante correo electrónico.

2. Propósito

El propósito de esta política de correo electrónico es para garantizar el uso adecuado del sistema de correo electrónico de la Organización y exponer a los usuarios acerca de lo que Trade Solutions estime como uso aceptable e inaceptable de su sistema de correo electrónico. Esta política describe los requisitos mínimos para el uso del correo electrónico dentro de la organización.

3. Alcance

Esta política contempla el uso apropiado de cualquier correo electrónico enviado desde una dirección de correo electrónico bajo el dominio de TradeSolutions.com y se circunscribe a todas las dependencias, instancias y entes que operan en nombre de Trade Solutions.

4. Políticas

4.1. Todo el uso del correo electrónico debe ser coherente con las políticas y procedimientos de conducta ética, la seguridad de los intereses de Trade Solutions como también en cumplimiento de las leyes y prácticas comerciales adecuadas aplicables.

4.2. Las cuentas de correo electrónico otorgadas bajo el dominio TradeSolutions.com o dependencias de la misma debe ser utilizada principalmente para los fines relacionados con sus actividades; se permite la comunicación personal en un ambiente limitado y restringido.

4.3. La organización Trade Solutions asegura y obliga a que los datos contenidos dentro de un mensaje de correo electrónico o un archivo adjunto deben ser asegurados de acuerdo a la Norma de Protección de Datos.

4.4. El correo debe mantenerse sólo si existe una razón para preservar la información contenida en el correo electrónico.

4.5. El Sistema de correo electrónico no se utilizará para la creación o distribución de mensajes que puedan llegar a ser perturbadores u ofensivos, que incluyan comentarios ofensivos acerca de la raza, el género, discapacidad, edad, orientación sexual, las creencias religiosas, creencias políticas, u origen nacional. Los empleados que reciban correos electrónicos o presenciara la distribución o creación de un correo con este contenido debe informar de ello a su supervisor inmediatamente.

4.6. Los usuarios tienen prohibido reenviar automáticamente e-mail a un tercer sistema de correo electrónico de terceros. Los mensajes individuales que se remiten por el usuario no debe contener información confidencial o superior.

4.7. Las cuentas de correo electrónico de Trade Solutions tendrán la siguiente denominación:

4.7.1. *Institucionales* asignadas a la alta gerencia.

4.7.2. *Dependencias* otorgadas a las diferentes dependencias u organizaciones dentro de la dirección de Trade Solutions

4.7.3. *Analistas* asignadas a los especialistas en inspección de punto de venta.

4.8. La organización Trade Solutions puede controlar y supervisar la emisión, almacenamiento y tratamiento de los mensajes relacionados con la cuenta de correo electrónico de la institución sin previo aviso.

4.9. La cuenta de correo electrónico es personal e intransferible, siendo responsabilidad exclusiva del usuario las acciones que se realicen con dicha cuenta, así como salvaguardar la clave de acceso asociada a su cuenta.

4.10. Toda cuenta de correo electrónico tendrá un único responsable. El uso de las cuentas de correo electrónico de *Dependencia* es responsabilidad del Jefe de la

dependencia a la cual fue asignada. Los responsables podrán autorizar el uso de dicha cuenta de correo electrónico a otra persona, sin eximirse de la responsabilidad por el cumplimiento de la presente política.

5. Cumplimiento de Políticas

Todo usuario que incumpla alguna de estas normas podrá estar sujeto a acciones administrativas o disciplinarias de acuerdo con el rol que cumple en la organización y con lo previsto en la reglamentación vigente correspondiente.

Cuando la conducta del usuario constituya un comportamiento tipificado como delito por las leyes de la República Bolivariana de Venezuela, éste asumirá la responsabilidad civil, patrimonial o penal correspondiente.

6. Estándares relacionados, Políticas y Procesos

Norma de Protección de Dato

7. Historias de las revisiones

Fecha del Cambio	Responsable	Resumen de los cambios
Julio, 2016	Carlos Rangel	Creación y adaptación

Políticas de Instalación de Software

1. Información general

El uso de herramientas que faciliten la realización de las tareas necesarias para alcanzar el objetivo de la empresa, es fundamental en toda organización, es por ello que es inevitable el uso de software especializado en los diferentes ámbitos de la organización, sin embargo, es importante mencionar que el uso inapropiado de software, expone a Trade Solutions contra riesgos legales y de seguridad informática, tales como la perdida de información, filtración de datos, infracción de derechos de autor, exposición de los sistemas internos a códigos maliciosos, interrupciones o degradación de servicios de red, suplantación de identidad, daños de sistemas, entre otros.

2. Propósito

El propósito de esta política proporcionar es informar, normar y regularizar el uso e instalación de software en Tade Solution, como también dar a conocer las reglas para la seguridad de equipos informáticos de Trade Solutions, con el fin de garantizar la seguridad de la información ubicada en las estaciones de trabajo de la organización. La política además proporciona una guía para garantizar los requisitos de la regla de seguridad de HIPAA referente a la seguridad de las estaciones de trabajo.

3. Alcance

Esta política se aplica a todos los trabajadores, contratistas, analistas y supervisores de puntos de venta y agentes que se desenvuelven en Trade Solutions. Aplicando directamente sobre las estaciones de trabajo de la organización y los equipos tecnológicos usados para llevar a cabo las tareas de la empresa.

4. Políticas

4.1. Es facultad exclusiva del Departamento de Tecnología de la Información realizar la instalación de software en los equipos propiedad de Trade Solutions.

4.2. Bajo ninguna circunstancia se permitirá al usuario realizar instalaciones de software, esto con el fin de garantizar el buen desempeño del software, el correcto funcionamiento de los ordenadores y la seguridad de la información de la organización.

4.3. Los requerimientos de instalación de software que no cuenten con una licencia valida, deberán ser canalizados formalmente a través del director de departamento al que está adscrito, quien deberá escalar al Departamento de Tecnología de la Información para analizar si existen alternativas de software libre, si es posible asignar una licencia disponible, o se gestiona la compra.

4.4. La solicitud de software especializado deberá ser solicitada al director del área a la cual el usuario corresponde. El director del área a su vez realizará la solicitud al Departamento de Tecnología de la Información, deberá incluir una lista de actividades a realizar con esta nueva herramienta.

4.5. Toda adquisición de software deberá ser acompañada de un dictamen hecho por el Departamento de Tecnología de la Información que avala la necesidad de la aplicación así como el cumplimiento de los criterios técnicos, de seguridad de la información y de usabilidad.

4.6. Trade Solutions y sus empleados no harán ni usarán copias no autorizadas de software de computadora. Bajo ninguna circunstancia Trade Solutions o un empleado de la organización usar software de computadora que no esté debidamente licenciado por el editor del software.

4.7. No se podrá instalar software protegido por derechos de autor, sin la respectiva licencia en los equipos computacionales propiedad de Trade Solutions, con la excepción de licencias que permitan su uso y distribución libre.

4.8. No se hará entrega de medios físicos o números de serie de licenciamiento a los usuarios que utilicen la licencia, por tratarse de información delicada y confidencial que tiene por objeto proteger los planes de licenciamientos y compromisos legales de Trade Solutions.

4.9. Con el objeto de evitar un consumo indebido de recursos de almacenamiento, de red y de computación, el Departamento de Tecnología de la Información realizará periódicamente tareas de revisión del software instalado, procediendo a tareas de actualización o desinstalación.

5. Cumplimiento de Políticas

Cuando la conducta del usuario constituya un comportamiento tipificado como delito por las leyes de la República Bolivariana de Venezuela, éste asumirá la responsabilidad civil, patrimonial o penal correspondiente.

6. Estándares relacionados, Políticas y Procesos

Políticas de contraseña

Política de cifrado en las estaciones de trabajo portátiles

Política de las redes y comunicaciones inalámbricas

Estándar de configuración de las estaciones de trabajo

7. Historias de las revisiones

Fecha del Cambio	Responsable	Resumen de los cambios
Agosto, 2016	Carlos Rangel	Creación y adaptación

Política de Credenciales de Base de Datos

1. Visión General

Las credenciales de autenticación de la base de datos son una parte necesaria que autoriza a la aplicación para conectarse a las base de datos internas. Sin embargo el uso incorrecto, almacenamiento y transmisión de tales credenciales, podrían comprometer los activos más sensibles y servir de eslabón para un compromiso mayor que engloba toda la organización.

2. Propósito

Esta política establece los requisitos para almacenar y recuperar los nombres de usuario y contraseñas (credenciales de base de datos) de forma segura para su uso por un programa (por ejemplo Tracking Tools) que tendrá acceso a una base de datos que se ejecuta en las redes de Trade Solutions.

Las aplicaciones de software que se ejecutan en las redes de Trade Solutions, pueden requerir el acceso a uno de los muchos servidores de base de datos internas. Con el fin de tener acceso a estas bases de datos, un programa debe autenticarse en la base de datos mediante la presentación de credenciales aceptables. Si las credenciales se almacenan de forma inadecuada, las credenciales pueden verse comprometidas, colocando en un compromiso a toda la base de datos.

3. Alcance

Esta política va dirigida a todo el personal que interactúa con el sistema, auditores y a los ingenieros del software quienes pueden desarrollar aplicaciones que tendrán

acceso al servidor de base de datos de la red de Trade Solutions. Esta política se aplica a todo el software (programas, módulos, librerías o APIS que accederán a la base de datos de Trade Solutions

4. Política

General

Con el fin de mantener la seguridad en las base de datos internas de Trade Solutions. El acceso a los programas de software debe ser concedido solo después de la autenticación con credenciales. Las credenciales utilizadas para la autenticación no deben residir en el cuerpo principal del programa, ejecutándose en el código fuente del mismo en texto plano. Las credenciales de base de datos no deben ser almacenadas en un lugar donde se pueda acceder a través de un servicio web.

Requerimientos Específicos

Almacenamiento de los nombres de usuario y contraseña en la base de datos

- Los nombres de usuario y contraseñas de la base de datos se deben almacenar en un archivo separado del código del cuerpo del programa en ejecución. Este archivo no debe ser legible por todo el mundo ni grabable.
- Las credenciales de la base de datos pueden residir en un servidor de base de datos. En este caso un número de identificación de una función hash de las credenciales puede ser almacenado en el cuerpo del código del programa en ejecución.
- Las credenciales de la base de datos pueden ser almacenadas como parte de un servidor de autenticación, tal como un servidor LDAP utilizado para la autenticación de usuario. La autenticación a la base de datos puede ocurrir en nombre de un programa como una parte del proceso del proceso de autenticación en el servidor. Es este caso, no es necesario el uso programático de las credenciales de la base de datos.

- Las credenciales de base de datos no pueden residir en el árbol de documentos de un servidor web.
- Pasar a través de la autenticación (es decir, Oracle OPS$ autenticación) no debe permitir el acceso a la base de datos únicamente basado en la autenticación de un usuario remoto desde un host remoto
- Las contraseñas o frases que se utilizan para acceder a una base de datos deben cumplir con la directiva de contraseñas.
- El personal de Trade Solutions con facultades de alterar los registros de la base de datos (auditorías, reportes entre otros) No deberá proporcionar sus credenciales a demás personal de la organización ni a auditores externos

La recuperación de los nombres de usuario y contraseña de la base de datos

- Si las credenciales se almacenan en un archivo que no es el código fuente, a continuación los nombres de usuario y contraseñas deben ser leídos del archivo inmediatamente antes de su uso. Inmediatamente después de la autenticación en la base de datos, la memoria que contiene el nombre de usuario y la contraseña debe ser liberada o borrada.
- El ámbito en el que es posible almacenar las credenciales de la base de datos debe ser separado físicamente de las otras áreas del código, por ejemplo, las credenciales deben estar en un archivo fuente independiente. El archivo que contiene las credenciales (nombre de usuario y contraseña) no debe contener ningún otro código, cualquier función, rutinas, o métodos que serán usados para acceder a las mismas.
- Para lenguajes que se ejecutan en el código fuente, el archivo de origen de las credenciales no debe residir en el mismo árbol de directorios de archivos navegables en el cual el código que se ejecuta reside.

Acceso a la base de datos de usuarios y contraseñas

- Cada programa o colección de programas que implementan una función de negocio deben tener una credencial única a la base de datos. No se permite el intercambio de credenciales entre los programas.
- Los auditores externos de Trade Solutions que proporcionarán constantemente información a la base de datos solo tendrán acceso a la misma bajo su única credencial y código de auditor, el cual será intransferible a personas externas que no encuentren relacionadas con la compañía.
- Las contraseñas utilizadas por los programas son las contraseñas a nivel de sistemas, como se define en la política de contraseñas
- Los grupos de desarrollo deben tener un proceso para asegurarse que las contraseñas de la base de datos se controlan y se cambian de acuerdo a la política de contraseñas de la empresa. Este proceso debe incluir un método para restringir el conocimiento de las contraseñas de la base de datos.

Técnicas de codificación para implementar esta política

- El equipo de desarrollo creará aplicaciones que contribuyan a los procesos internos de la organización y facilite los reportes hechos por los auditores manteniendo los estándares de seguridad de la empresa
- Las aplicaciones dirigidas a los auditores de Trade Solutions serán de entorno web, las mismas tendrán un continuo monitoreo de sus credenciales y acceso a las base de datos de Trade Solutions
- El lenguaje de programación utilizado por el equipo de desarrollo será discutido e implementado bajo su criterio siempre que se adapte a esta política de seguridad.

5 Cumplimiento de Política

5.1 Medición del Cumplimiento

El equipo de seguridad de la información verificará el cumplimiento de esta política a través de varios métodos, incluyendo pero no limitado a los reportes de la herramienta de negocio, auditorías internas y externas y la retroalimentación con el dueño de la política.

5.1 Excepciones

Cualquier excepción a la norma debe ser aprobada por el equipo de seguridad de la información con antelación

5.2 Incumplimiento

Un empleado que haya violado esta política debe estar sujeto a medidas disciplinarias, incluyendo incluso la terminación de su empleo.

Una violación de esta política por un trabajador temporal, contratista o proveedor puede resultar en la terminación de su contrato con Trade Solutions

Cualquier código de programa o aplicación que se encuentre violando esta política deben ser remediados en un periodo de 90 días

6 Estándares Relacionados, Políticas y Procesos

Política de Contraseña

Términos empleados

- Credenciales
- Cuerpo en ejecución
- Función Hash
- LDAP

- Módulo

Historia de Revisión

Fecha de Cambio	**Responsable**	**Resumen de Cambios**
Agosto 2016	Tyson Cardelli	Creación y Adaptación