TÍTULO: Transferencia de Archivos con Terceros

Código: SI 14 001 Versión: 1 Vigencia: 01/06/2017

1- OBJETIVOS

- Establecer las pautas relativas a la transferencia de archivos requeridos por el negocio de la compañía en ambas direcciones: desde la empresa al tercero y del tercero a la empresa.
- Contar con un marco seguro y confiable para el intercambio de archivos en particular los confidenciales.
- Evitar el envío y reenvío de archivos a través de mecanismos no apropiados, por ejemplo el correo electrónico (email). El peso de estos archivos por lo general es grande, con lo cual afectan directamente a la performance de los servidores y comunicaciones de ENVASES DEL PLATA. Ya sea ocupando espacio en disco innecesario, como ocupando el ancho de banda disponible para la empresa. Se generan N copias de los archivos las cuales quedan desperdigadas en N clientes y servidores de correo electrónico, haciendo más dificultosa la tarea de trabajo colaborativo.
- Contar con un esquema de accesos y permisos a los archivos que sea controlado. Manejando tiempos de expiración, ABM de usuarios, etc.

2- ALCANCE

Esta política inicialmente esta cubriendo las necesidades de sectores especiales de la compañía (Desarrollo, Dirección) y los clientes de la compañía de todo tamaño.

En virtud de que la presente política surge como resultado de la aplicación de procedimientos que están en uso de hace unos años, se cuenta con la experiencia y conocimiento necesario como para que estas herramientas puedan ser usadas por otros sectores que requieran transferir información en formato seguro.

3- DESCRIPCIÓN

Se configuró e implementó un esquema de Secure File Transfer orientado a la transmisión de forma segura, práctica y eficiente de archivos entre las distintas áreas de Desarrollo y sus correspondientes clientes o estudios de diseño.
Se definieron dos tipos de usuarios A y B.
Básicamente esta diferenciación radica en la importancia y periodicidad de trabajo con los distintos clientes y sus estudios de diseño. Ambas soluciones están preparadas para ser escaladas en caso de que sea necesario.
El objetivo principal del sistema es hacer más seguras y eficientes las transferencias de archivos entre las partes en cuestión.

a. Usuarios tipo "A"

Para los usuarios del tipo "A" se implementó la solución de Secure File Transfer de Accellion for Business (http://www.accellion.com).

Esta solución cuenta con las siguientes características:

- De 5 a 500 Usuarios (en paquetes de 5, 10, 25, 50, 100, 200, 300, 400, 500).
- 1000 GB de almacenamiento de archivos en línea.
- Archivos de 2 GB máximo.
- Implementación en la nube.
- Sincronización de archivos y uso compartido.
- Asegure los Links para compartir archivos.
- Kitedrive (sincronización continua de escritorio).
- Aplicaciones móviles - iPhone, iPad, Android, Blackberry.
- Proyecto / Equipo de Colaboración.
- Asegure los espacios de trabajo de grupo en línea.
- Sincronización de espacio de trabajo.
- Acceso basado en roles.
- Seguimiento de versiones de archivo.
- Archivos Comentados.
- Administración de IT, Audit Trail y controles de seguridad.
- Almacenamiento de archivos cifrados.
- Transferencia segura de archivos.
- Seguimiento Integral de archivos.
- Branding personalizado.
- Soporte Online y telefónico (USA).

b. Usuarios tipo "B"

Para los usuarios del tipo "B" se implementó una solución de "Hosting Shared".
Esta solución cuenta con las siguientes características:

- Almacenamiento en disco ilimitado.
- Transferencia ilimitada.
- Acceso FTP y SFTP.
- Archivos pre-configurables e instructivos de los siguientes clientes de FTP: Filezilla y Core FTP (Windows) y Cyberduck (Mac).
- Secure Shell (SSH) Acceso.
- Acceso vía "disco de red" con "drag & drop" con instructivos para los diferentes sistemas operativos.
- Archivos de registro.
- Cronjobs personalizados.
- Servidor seguro SSL.
- Directorios protegidos con contraseña.
- Tecnología de clase mundial.
- Sistema Operativo Linux.
- Red 24/7 Monitoreo.
- Varias conexiones 10 Gigabit Ethernet.

c. Manejo de excepciones

En el caso que se requieran excepciones para cualquiera de los puntos anteriores, se deberán cumplir con los puntos siguientes.

1. Deberá estar solicitada por correo electrónico por el gerente del área solicitante, contendrá la justificación del pedido y toda la información que sea requerida por el área de Sistemas.
2. Sistemas evaluará la factibilidad técnica del pedido, en caso afirmativo enviará un correo electrónico a la Dirección General[1] con su informe positivo. En caso negativo seguirá el mismo proceso anterior justificando los motivos técnicos por los cuales se rechaza el pedido.
3. En caso afirmativo, la solicitud deberá ser aprobada por la Dirección General, quien responderá por el mismo medio.
4. Sistemas definirá para cada caso las condiciones de "seguridad requeridas", en un todo de acuerdo con las políticas y la auditoria. En caso de no poder satisfacer la solicitud o de auditarse una falla potencial de seguridad, se rechazará el pedido por razones técnicas (hasta tanto puedan ser superadas).
5. Sistemas documentará todas las excepciones aprobadas contando para ello con toda la información que se requiera según el caso (ej: solicitante, motivo de la solicitud, tipo de acceso, personas, roles, lugar de acceso, sistemas a los que acceden, tiempo durante el cual tiene que estar habilitado, etc.) y tendrá copia firmada digitalmente de la aprobación gerencial.
6. Si se detectara el incumplimiento de alguna de estas condiciones, el proceso automático indica que Sistemas primero cancela la excepción y luego informa a los participantes (Gerencia solicitante y Dirección General) para su revisión.
7. Se mantendrá un registro preciso y continuo de todas las excepciones.

4- RESPONSABILIDAD y CONTROL

Los responsables del cumplimiento de lo expresado serán cada una de las Gerencias y Direcciones y los controlantes serán el área de Sistemas y la auditoría externa de la compañía. Para asegurar el cumplimiento se realizarán verificaciones periódicas, monitoreos y auditorías aleatorias.

5- DISPOSICION

El incumplimiento de cualquiera de los puntos detallados implicará una violación a la seguridad de la información de EPSA, haciendo directamente responsable a la persona que hubiese incurrido en el mismo. En el caso que corresponda será también responsable el ejecutivo responsable del área en la que se hubiese determinado un problema de seguridad.

6- HISTORICO DE CAMBIOS

[1] o a quién ésta delegue

Confeccionó: Juan M. Ferraro / C.Lozano	Revisó: Jorge Barreiro	Aprobó: Martín Guaita
Firma	Firma	Firma
COMITÉ DE SI	GERENCIA DE SISTEMAS	GERENCIA GENERAL