TÍTULO: Especificaciones sobre Seguridad

Código: SI 12 001 Versión: 2 Vigencia: 01/10/2014

1- OBJETIVOS

- Recalcar las exigencias de seguridad que deben ser observadas por las direcciones, gerencias, ejecutivos y empleados.
- Remarcar los objetivos planteados y en plena ejecución que en cuanto a Seguridad de la Información viene llevando adelante la compañía.
- Aclarar los procedimientos, marcar las responsabilidades e identificar a los responsables tanto del cumplimiento como del control.
- Contar con herramientas que además de incrementar la seguridad, permitan prever fallas y en caso de no ser factible, detectarlas y corregirlas en el menor tiempo posible.
- Disponer de pistas de auditoria para la identificación de los responsables de violaciones de seguridad.

2- ALCANCE

Esta política reúne conceptos de otras políticas en vigencia, elaboración o redacción y surge como necesidad de sintetizar y enfatizar los objetivos planteados previamente.

3- DESCRIPCIÓN

a. Políticas

1. Todas y cada una de las políticas publicadas por la compañía son de cumplimiento obligatorio sin excepciones.
2. A la fecha hemos firmado las siguientes:
    - SI 01 001 – Escritorios Limpios
    - SI 02 001 – Passwords
    - SI 03 001 – Acceso Lógico
    - SI 05 001 – Correo Electrónico
    - SI 06 001 – Seguridad del Equipamiento Informático y los Sistemas de Comunicación de Datos
    - SI 07 001 – Acceso de Terceros a las Instalaciones
    - SI 08 001 – Uso de Internet
3. Se encuentran a la firma:
    - SI 13 001 – Procedimiento de Contingencia de SAP
4. Se encuentran en redacción y revisión las siguientes:
    - SI 04 001 – Documentación
    - SI 09 001 – Computación Móvil y Teletrabajo
    - SI 10 001 – Terceros
    - SI 11 001 – Seguridad en Planta
5. Se continuará en esta misma dirección y de acuerdo al plan en vigencia hasta completar el Manual de Políticas de EPSA.

b. Passwords

1. Todas las passwords deben indefectiblemente tener período de expiración.

2. La password es individual y no se debe pasar bajo ningún concepto. Si existe alguna excepción (reemplazo por vacaciones, etc.), debe cambiarse al revertirse la situación.
3. Todos los equipos deben indefectiblemente tener activado el bloqueo automático cuando estén sin uso por más de 10 minutos.
4. Para facilitar el manejo y asegurar el acceso, se emplearán lectores de huellas digitales, los que se instalarán y pondrán en producción durante el corriente mes.

c. Archivos

1. En todos los casos los archivos deben ser guardados en las carpetas asignadas en los servidores. No se debe conservar ninguna información confidencial en las PC o laptops.
2. Los permisos de acceso han sido definidos y revisados por cada gerencia de acuerdo a sus necesidades. Si los gerentes dan acceso a otras personas, se hacen responsables de las posibles violaciones de seguridad.
3. Para el almacenamiento de archivos en formato "temporal" existe una carpeta "pública" que no requiere la asignación de permisos por parte de Sistemas.
4. El objetivo de esta carpeta pública es poder acceder sin restricciones a un espacio común de almacenamiento.
5. Se destaca que la información en esa carpeta será "limpiada o eliminada" por Sistemas con una frecuencia de seis (6) meses a los efectos de mantener la capacidad de almacenamiento dentro de niveles razonables.
6. Sistemas notificará vía email a todos los interesados respecto a la fecha de borrado de archivos.
7. Es responsabilidad de cada Gerencia (y por ende de los usuarios dentro de cada una de ellas), mantener la información dentro de las carpetas asignadas correspondientes, moviendo, si corresponde, de la carpeta pública a la asignada. Recalcándose que a ésta última sólo acceden las personas autorizadas por cada Gerencia.
8. La trasmisión de archivos confidenciales se deberá realizar de modo seguro, en particular con terceros. Para ello la compañía dispone de herramientas adecuadas. Ante esta necesidad por favor comuníquese con Sistemas para que le indiquen el método apropiado.

d. Correo Electrónico

1. No se deben enviar sistemáticamente archivos adjuntos en los correos electrónicos, para ello se debe reemplazar por un link indicando el "path" donde reside el archivo. El lugar de residencia del archivo deberá cumplir con la política respectiva.
2. Se implementará, para los niveles que corresponda, el uso de certificados digitales para firma y cifrado de correo electrónico. Esto aplica especialmente para la información confidencial. Esto asegurará: Autenticidad, Inalterabilidad, Confidencialidad y No repudio.
3. En primera instancia se instalarán estas facilidades para los Directores, luego de estabilizado el procedimiento se extenderá a Gerentes y otros usuarios que por sus funciones requieran de esta función de seguridad.
4. La información confidencial sólo deberá trasmitirse mediante canales seguros estando prohibido el uso de teléfonos celulares, PDA's o dispositivos similares para dichos fines. La persona que envíe información confidencial por estos canales no seguros se hace totalmente responsable ante una falla de seguridad.

e. Hardware y Software

1. Está prohibida la conexión de cualquier dispositivo externo (pen drive, cámaras, celulares, etc.) que no hayan sido provistos por la compañía.
2. Lo mismo aplica para cualquier tipo de software no provisto por la empresa.

f. Conexiones Remotas

1. Como política general están prohibidos los accesos remotos.
2. En el caso de ser requerido a partir de una necesidad concreta de la compañía se deberá definr un ingreso que emplee una VPN con IP filtrado.
3. En todos los casos, tanto Sistemas como la Auditoria Externa implementará y deberá contar con las funcionalidades de auditoría y registro de eventos para un correcto control.

g. Administración de dominios

1. Existirá un solo usuario y grupo administrador de dominio, con los mecanismos de resguardo correspondientes.
2. Cualquier tipo de requerimiento deberá ser ejecutado y documentado por dicho administrador.
3. Todos los usuarios que requieran permisos administrativos serán agregados al grupo administrador, deberán sólo contar con el acceso que sea requerido y por tiempo establecido, caducando los mismos a su vencimiento.
4. Se mantendrán activas todas las funcionalidades de auditoria y registro de eventos en todos los servidores de la compañía para un correcto control.

h. 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[1] 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[2] 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.

---

[1] cada correo electrónico en estos circuitos deberá estar firmado digitalmente

[2] o a quién ésta delegue

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- ANEXOS

Se adjuntan los siguientes anexos a la presente política:

1. Diagrama Acciones IT
2. Escalamiento de Incidentes IT
3. Escalamiento de Incidentes SAP
4. Tareas y responsables IT
5. Manejo de excepciones

6- 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.

7- HISTORICO DE CAMBIOS

a. Primera revisión: 01.04.2011
b. Segunda revisión: 02.05.2013
c. Tercera revisión: 02.10.2014

Confeccionó: JM.Ferraro	Revisó: J. Barreiro	Aprobó: M. Guaita
Firma	Firma	Firma
COMITÉ DE SI	GERENTE DE SISTEMAS	GERENCIA GENERAL