emape s.a.
EMPRESA MUNICIPAL
ADMINISTRADORA DE PEAJE DE LIMA

POLITICAS DE SEGURIDAD DE INFORMACION

Versión: 001	Código: GCPS-GSI-007-2015	Fecha: 14/08/2015	Nº. Páginas: 10

GSI - SOPORTE TECNICO - GCPS
VºBº
EMAPE S.A.

Rubro	Nombre	Cargo	Firma
REVISADO POR	Rubén Yépez Moreano	Gerente de Sistemas de Información	
APROBADO POR	Hugo Contreras Chávez	Gerente Central de Planeamiento y Sistemas	

1. OBJETIVO

Establecer normas para la seguridad de la información institucional almacenada en los equipos informáticos de EMAPE.S.A.

2. FINALIDAD

- Proteger la información administrada en los equipos informáticos de EMAPE.S.A.
- Garantizar la continuidad del servicio informático en las diversas áreas de EMAPE.S.A.
- Establecer las responsabilidades de los usuarios, en relación con la información que utilizan.

3. ALCANCE

Esta Politica es de alcance a todo usuario de las Gerencias de EMAPE.S.A., que tenga acceso al servicio de equipos de cómputo y equipos de comunicación que almacenen información institucional.

4. BASE LEGAL

- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley Nº 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM), modificada por Ley Nº 29246 y su Reglamento, aprobado por Decreto Supremo Nº 031-2005-MTC.
- Ley Nº 28612 que norma el uso, adquisición y adecuación del software de la Administración Pública.
- Ley Nº 29151, Ley General del Sistema Nacional de Bienes Estatales y su Reglamento, aprobado por Decreto Supremo Nº 007-2008-VIVIENDA
- Decreto Legislativo N° 1057 "Decreto Legislativo que Regula el Régimen Especial de la Contratación Administrativa de Servicios".
- Resolución Jefatural N° 088-2003-INEI, que aprueba Directiva N° 005-2003-INEI/DTNP sobre "Normas para el uso del servicio de correo electrónico en las entidades de la administración pública"
- Resolución de Contraloría Nº 320-2006-CG que aprueban Normas de Control Interno.
- Resolución Ministerial N° 246-2007-PCM "NTP-ISO/IEC 17799:2007 EDI Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición".
- Decreto Supremo Nº 013-2003-PCM, Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.

- Resolución Ministerial Nº 073-2004-PCM, Aprueban Guía para la Administración Eficiente del Software Legal en la Administración Publica.

- Resolución de Contraloría Nº 072-98-CG, Normas Técnicas de Control Interno para Sistemas Computarizados, Codificada como Norma 500-01 al 500-08.
- Norma Técnica Peruana, "NTP-ISO/IEC17799:2004 EDI - Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 1ª Edición".

- Reglamento de Organización y Funciones vigente.

5. JUSTIFICACION

La masiva utilización de recursos informáticos (Computadores, impresoras, redes de datos, etc.) Como medio para almacenar, transferir y procesar información, se ha incrementado desmesuradamente en los últimos años, al grado de convertirse en un elemento esencial para el funcionamiento de la sociedad y de las diferentes Empresas.

En consecuencia, la información, y por consiguiente los recursos mencionados anteriormente, se han convertido en un activo de altísimo valor, de tal forma que, EMAPE SA no puede ser indiferente y por lo tanto, se hace necesario proteger, asegurar y administrar la información para garantizar su integridad, confidencialidad y disponibilidad, de conformidad con lo establecido por la ley.

En los últimos años se ha incrementado el uso de aplicaciones electrónicas que comprenden: correo electrónico, internet, transacciones, firmas y certificados digitales, comunicaciones seguras, entre otras. Por tal motivo, los requerimientos de seguridad son cada vez mayores.

6. DEFINICIÓN

La seguridad informática aplica las técnicas fundamentales para preservar la información y los diferentes recursos informáticos con que cuenta EMAPE S.A. La política de seguridad informática es el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada, al igual que garantizan la conservación y buen uso de los recursos informáticos con que cuenta EMAPE SA.

7. GLOSARIO

Para efectos del presente documento se entiende por:

Administrador del sistema. Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está en cabeza del área de Sistemas.

Administrador de correo. Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.

Buzón. También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a EMAPE SA.

Chat. (Tertulia, conversación, charla). Comunicación simultánea entre dos o más personas a través de Internet.

Computador. Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Contraseña o password. Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Correo electrónico. También conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

Cuentas de correo. Son espacios de almacenamiento en un servidor de correo, para guardar información de correo electrónico. Las cuentas de correo se componen de un texto parecido a este sistemas@emape.gob.pe donde "sistemas" es nombre o sigla identificadora de usuario, " emape " el nombre EMAPE SA con la que se crea la cuenta o el dominio y ".gob.pe" una extensión propio de Internet según el dominio.

Edición de cuentas de correo. Mirar o leer el contenido de los correos recibidos o enviados por un usuario.

Downloads. Descargar, bajar. Transferencia de información desde Internet a una computadora.

Electricidad estática. La corriente estática se presenta cuando no existe ninguna fuerza externa (voltaje) que impulse a los electrones o si estos no tienen un camino para regresar y completar el circuito, la corriente eléctrica simplemente "no circula". La única excepción al movimiento circular de la corriente la constituye la electricidad estática que consiste enel desplazamiento o la acumulación de partículas (iones) de ciertos materiales que tienen la capacidad de almacenar una carga eléctrica positiva o negativa.

Elementos de tecnología. Se consideran los siguientes, siendo la Gerencia de Informática responsable de su administración.

- Computadores de escritorio y portátiles: conformados por CPU (Discos duros, memorias, procesadores, main borrad, bus de datos), cables de poder, monitor, teclado, mouse.
- Impresoras, UPS, escáner, lectores, fotocopiadoras, teléfonos, radioteléfonos.
- Equipos de redes comunicaciones como: Switch, router, Hub, Conversores de fibra y demás equipos de redes y comunicaciones.

Hacker. Persona dedicada a lograr un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red con el objeto de alterar en forma nociva su funcionamiento.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet. Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que solo es de uso interno.

Lan. (Local Area Network). (Red de Area Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Log. Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoría.

Megabyte MB. Es bien un millón de bytes ó 1.048.576 bytes.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Seguridad: Mecanismos de control que evitan el uso no autorizado de recursos.

Servidor. Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de correo. Dispositivo especializado en la gestión del tráfico de correo electrónico. Es un servidor perteneciente a la red de Internet, por lo que tiene conexión directa y permanente a la Red Pública. Su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

S.O. (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software. Todos los componentes no físicos de una PC (Programas).

Usuario. Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de EMAPE SA debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

Virus. Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que sonutilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya y gusano).

Monitoreo de Cuentas de correo. Vigilancia o seguimiento minucioso de los mensajes de correo que recibe y envía un usuario.

Web Site. Un Web Site es equivalente a tener una oficina virtual o tienda en el Internet. Es un sitio en Internet disponible para ser accesado y consultado por todo navegante en la red pública. Un Web Site es un instrumento avanzado y rápido de la comunicación que facilita el suministro de información de productos o entidades. Un Web Site es también considerado como un conjunto de páginas electrónicas las cuales se pueden accesar a través de Internet.

Web Mail. Es una tecnología que permite acceder a una cuenta de Correo Electrónico (E-Mail) a través de un navegador de Internet, de esta forma podrá acceder a su casilla de correo desde cualquier computadora del mundo.

8. POLITICAS ADOPTADAS

EMAPE S.A., se encuentra dentro un Sistema de Gestión de la Calidad, y teniendo en cuenta que a través del Proceso de Soporte Informático se propone Administrar, desarrollar y mantener en buen estado los TICs, garantizando el apoyo logístico para el buen desarrollo de la Gestión; se adoptan las siguientes políticas de seguridad informáticas en EMAPE SA:

1. Cuentas de Usuarios
2. Internet
3. Correo Electrónico
4. Red Interna
5. Políticas de uso de computadores, impresoras y periféricos
6. Otras Políticas

Mucho se ha hablado de las mejores prácticas que debemos tener para resguardar nuestra organización con respecto al uso de los recursos informáticos, tales como el correo electrónico, redes y de internet. Hay discusiones sobre confidencialidad, propiedad de la información transmitida en los mensajes, códigos de ética y privacidad del correo.

Hemos realizado un listado de pautas que se deben tener en cuenta para dar un uso adecuado a los recursos informáticos (correo electrónico, red interna, internet) provisto por EMAPE S.A.:

El área de sistemas auditará de manera periódica los equipos de cómputo y periféricos así como el software instalado.

El propósito de estas políticas es asegurar que los funcionarios utilicen correctamente los recursos tecnológicos que EMAPE SA pone a su disposición para el desarrollo de las funciones institucionales.

Dichas políticas son de obligatorio cumplimiento.

El funcionario, empleado que incumpla las políticas de seguridad informática, responderá por sus acciones o por los daños causados a la infraestructura tecnológica de EMAPE S.A, de conformidad con las leyes penales, fiscales y disciplinarias.

1. Cuentas de Usuarios

Es la cuenta que constituye la principal vía de acceso a los sistemas de información que posee EMAPE SA; estas cuentas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema o a otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros.

Cada persona que acceda al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control, evita

Una cuenta de usuario asigna permisos o privilegios al usuario para acceder a los sistemas de información y desarrollará actividades dentro de ellas. Los

privilegios asignados delimitan las actividades que el usuario puede desarrollar sobre los sistemas de información y la red de datos.

Procedimiento para la creación de cuentas nuevas:

La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por el formulario digital y ser debidamente autorizada por el Gerente de la Oficina que lo requiere.

No debe concederse una cuenta a personas que no sean funcionarios o empleados de EMAPE S.A, a menos que estén debidamente autorizados.

Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye a los administradores del sistema.

La Oficina de RRHH debe reportar a la Oficina de Sistemas, de los funcionarios que cesan sus actividades y solicitar la desactivación de su cuenta.

No se otorgará cuentas a técnicos de mantenimiento externos, ni permitir su acceso remoto, a menos que la Gerencia de Sistemas de Información y Comunicación de determine que es necesario.

En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).

No se crearán cuentas anónimas o de invitado.

2.Internet

Internet es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas. Se debe aplicar una política que procure la seguridad y realizar monitoreo constante, por lo que se debe tener en cuenta lo siguiente:

A continuación se describen las políticas adoptadas para el uso adecuado de este importante servicio:

No acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista etc. o que estén fuera del contexto laboral.

En ningún caso recibir ni compartir información en archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus al equipo.

No descargar programas, demos, tutoriales, que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado. La descarga de ficheros, programas o documentos que contravengan las normas de la Institucion sobre instalación de software y propiedad intelectual.

Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo a la Gerencia de Sistemas de Información y Comunicación que se encargará de realizar las operaciones oportunas.

Los empleados de la Institución tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.

Ningún empleado debe instalar ningún programa para ver vídeos o emisoras de televisión vía Internet y de música. (Ares, REAL AUDIO, BWV, etc.).

No debe usarse el Internet para realizar llamadas internacionales (Dialpad, skipe, NET2PHONE, FREEPHONE, etc.).

3. Correo electrónico

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta Es de anotar que el correo electrónico es un instrumento de comunicación de EMAPE SA y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

A continuación se relacionan las políticas:

Utilizar el correo electrónico como una herramienta de trabajo, y no como nuestra casilla personal de mensajes a amigos y familiares, para eso está el correo personal.

No enviar archivos de gran tamaño a compañeros de oficina. Para eso existe la red.

No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas. Los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios en Internet.

No participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.

No distribuir mensajes con contenidos impropios y/olesivos a la moral. No enviar grandes cadenas de chistes en forma interna.

Si se recibe un correo de origen desconocido, consulten inmediatamente con la Gerencia de Sistemas de Información y Comunicación sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).

Cuando se contesta un correo, evitar poner "Contestar a todos" a no ser que estemos absolutamente seguros que el mensaje puede ser recibido por "todos" los intervinientes.

El acceso a las cuentas personales debe ser mínimo (o ninguno) durante nuestra jornada laboral.

Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.

Cuando el usuario deje de usar su estación de trabajo deberá cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo. Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.

Se debe eliminar permanentemente los mensajes innecesarios.

Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.

Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.

Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.

Evite enviar mensajes a listas globales, a menos que sea unasunto oficial que involucre a toda la institución.

La Gerencia de Sistemas de Información y Comunicación determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.

Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en el archive de extension PST ubicado en carpetas personales de la PC local.

4. Red Interna (INSTITUCIONAL)

INSTITUCIONAL es un recurso compartido para todos los empleados de EMAPE S.A. solo de uso laboral (compartir y almacenar información solo pertinente a sus tareas), no para almacenar cosas personales.

A la información guardada por los funcionarios EMAPE SA en la Red Interna se le realizarán copias de seguridad todos los viernes al finalizar la jornada laboral en un medio de almacenamiento externo; esto para proteger todo cuanto se guarde en esta carpeta compartida y así y tenerrespaldo de los datos.

En el servidor de red de la Institución existe un Servidor de Archivos con carpetas compartida denominada con los nombres de las Gerencias dentro de la cual hay una donde cada Sub Gerencia tendrá una subcarpeta para guardar los archivos

que desee compartir y a la cual tendrán acceso los empleados que el Gerente respectivo considere pertinente, también contará con una subcarpeta denominada común a la cual tendrán acceso todos los empleados pero esta se evacuará todos los viernes para así liberar espacio en disco evitando que este se mantenga lleno de archivos innecesarios.

Si guardó una información en la red y más adelante ya no es necesario tenerla allí, debe eliminarse y guardarla ya sea en el equipo, o en memorias cds etc. Para no mantener la red llena de cosas innecesarias.

No utilizar la red con fines propagandísticos o comerciales.

No modificar ni manipular archivos que se encuentren en la red que no sean de su propiedad, uso personal ni material innecesario.

5. Políticas de uso de computadores, impresoras y periféricos

La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.

Los usuarios no pueden instalar, suprimir o modificar el software originalmente No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia de la Gerencia de Sistemas de Información y Comunicación, el retiro o cambio de partes.

No es permitido destapar o retirar la tapa de los equipos, por personal diferente a la Gerencia de Sistemas de Información y Comunicación o bien sus asistentes o sin la autorización de esta, dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin previa autorización de la Gerencia de Sistemas de Información y Comunicación.

Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.
Es estrictamente obligatorio, informar oportunamente a la Gerencia de Sistemas de Información y Comunicación la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos. El reporte de las novedades debe realizarse a la Gerencia de Sistemas de Información y Comunicación tan pronto se presente el problema.

Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.

Los protectores de pantalla y tapiz de escritorio, serán establecidos por la Gerencia de Sistemas de Información y Comunicación y deben ser homogéneos para todos los usuarios.

Ningún funcionario, podrá formatear los discos duros de los computadores. Ningún funcionario podrá retirar o implementar partes sin la autorización de la Gerencia de Sistemas de Información y Comunicación.

6. Otras Políticas

A los equipos portátiles personales no se les brindará soporte de ninguna índole: ni de hardware ni de software, porque no son responsabilidad de la entidad por ende el dueño debe hacerse cargo y responsable de su computador. La dirección IP asignada a cada equipo debe ser conservada y no se debe cambiar sin la autorización de la Gerencia de Sistemas de Información y Comunicación porque esto ocasionaría conflictos de IP'S y esto alteraría el flujo de la red.

No llenar el espacio de disco del equipo con música ni videos, ni información que no sea necesaria para el desarrollo de sus tareas con respecto a la entidad.

Todo funcionario responsable de equipos informáticos debe dejarlo apagado y desenchufado tanto al medio día como en la noche lo anterior para ahorrar recursos energéticos y contribuir a la conservación de los equipos.