EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.

CÓDIGO: MAGI-01

VERSIÓN: 07

FECHA: 27/11/2018

MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

CUADRO CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del Cambio**
00	28/05/2010	Emisión inicial
01	25/02/2013	Actualizaciones generales a los capítulos que componen este manual
02	20/11/2013	Actualizaciones generales a los capítulos que componen este manual
03	12/02/2016	Actualizaciones generales a los capítulos que componen este manual
04	22/12/2016	Se incluye pie de página de copia No Controlada.
05	17/08/2017	Actualización del nombre del área de Sistemas de Información e inclusión de Políticas de Uso de Dispositivos de Almacenamiento Externo y Políticas de Navegación en Internet.
06	24/11/2017	Actualización que aplica la exclusión de soporte y mantenimiento a los Aplicativos Técnicos los cuales no son Administrados por el Proceso de Gestión Informática.
07	27/11/2018	Actualizaciones de Inactivación de cuentas y Actualización en la herramienta de gestión seleccionada del área de sistemas para su uso.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la Empresa y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión.

Para que estos principios de Seguridad de la Información sean efectivos, resulta necesaria la implementación de Políticas que forme parte de la cultura organizacional de la Empresa, lo que implica que debe contarse con el compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento de las mismas.

La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Empresa en materia de seguridad.

Es así, como la Administración General de EMPAS S.A provee a Directivos, Funcionarios, Empleados y Trabajadores, de medios técnicos e informáticos con herramientas de trabajo que garantizan la rapidez y eficacia en la prestación de sus servicios de acuerdo a sus actividades.

Entre estos medios se incluyen los equipos, programas y sistemas que facilitan el uso de las herramientas informáticas, el acceso a una red interna o intranet y una red externa o internet, así como la utilización de un buzón de correo electrónico o e-mail y teléfono.

Los sistemas de información deben servir para facilitar y agilizar la tramitación de los procedimientos administrativos, operativos, comerciales y de proyectos, asegurando la disponibilidad, autenticidad, confidencialidad e integridad de la información para la toma de decisiones y por ende el buen funcionamiento de la empresa.

El uso constante de los sistemas debe constituir la regla general de comportamiento de todos los integrantes de EMPAS S.A, no quedando, tal uso a potestad y criterio de sus usuarios.

Como resultado de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente de amenazas.

Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad y por lo tanto sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una "cultura de seguridad".

En virtud de las competencias de la Gerencia General sobre la administración de los bienes tangibles e intangibles de la Empresa, en este documento se establecen Políticas y Estándares de Seguridad de la Información.

2. CONCEPTOS FUNDAMENTALES

Disponibilidad: Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Confidencialidad: Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. A groso modo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a *integridad referencial* en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Autenticación: Es la propiedad que me permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados por la Empresa o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Empresa, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Responsable de Seguridad Informática: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

3. OBJETIVOS

Proteger los recursos de información de EMPAS S.A y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestales correspondientes.

Fomentar una cultura de seguridad informática mediante la socialización de las políticas a los usuarios para proteger los sistemas de información.

Incrementar la concientización sobre el riesgo de no dar uso adecuado a los sistemas de información, así como la necesidad de adoptarlos e implementarlos.

Establecer reglas precisas que determinen la mayor eficiencia en la seguridad de los sistemas de información de EMPAS S.A, evitando aquellas prácticas que supongan la utilización incorrecta o inadecuada de los sistemas de información.

Comprometer a todos los Usuarios de las Tecnologías de la Información a implementar principios básicos como conciencia y responsabilidad sobre la seguridad y manejo de la información.

4. NATURALEZA Y FINALIDAD

El presente Manual de Administración de Tecnología de la Información está dirigido a garantizar la seguridad de los sistemas de información en EMPAS S.A y de los activos que la sustentan.

5. ALCANCE

El documento describe las políticas y los estándares de seguridad que deberán observar de manera **obligatoria todos los usuarios** para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos de EMPAS S.A.

Se establecen las Políticas y Estándares de Seguridad de la Información, teniendo en cuenta que cada usuario es un actor importante para garantizar la seguridad, por lo que cada uno, de acuerdo a las funciones que desempeña, deberá estar consciente de los riesgos y de las medidas preventivas pertinentes, deberá asumir la responsabilidad correspondiente y tomar las medidas que permitan fortalecer la seguridad de los sistemas de información.

6. VIGENCIA

El presente documento estará vigente desde su publicación.

7. SANCIONES EN CASO DE VIOLACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACION

En el caso de que se constate alguna violación de las normas establecidas por la presente política de seguridad, se aplicará lo dispuesto en la ***ley 734 de 2002***, por el incumplimiento de los Deberes contenidos en el Art. 34 numerales 1, 2, 4, 5, 7, 11, 21, 22, 24 y 25, y **Ley 1273 de 2009** Delitos Informáticos.

8. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD LÓGICA

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de EMPAS S.A, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de EMPAS S.A., debe ser proporcionado por el dueño de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

8.1 Controles de Acceso Lógico

Todos los usuarios de servicios de información son responsables por el usuario y contraseña que recibe para el uso y acceso de los recursos.

Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Área de Sistemas de Información antes de poder usar la infraestructura tecnológica de EMPAS S.A.

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de EMPAS S.A., a menos que se tenga el visto bueno del dueño de la información y del Área de Sistemas de Información.

Cada usuario que acceda a la infraestructura tecnológica de EMPAS S.A debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.

Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el UserID de otros usuarios.

El Área de Sistemas de Información establecerá las medidas y normas oportunas para restringir los accesos de los empleados a los recursos informáticos solicitados, en los casos de vacancias temporales superiores a tres días donde el usuario se encuentre en un estado cesante, el asesor del área de Gestión Humana notificará al correo de ayuda@empas.gov.co la novedad correspondiente, el tiempo de inactivación tanto de la cuenta de acceso como del correo electrónico, el nombre del Servidor Público que resulte Encargado para asumir las funciones mientras exista la situación que generó el Control de Acceso a fin de proceder desde el área de sistemas quienes procederán a las actividades correspondientes. En los casos de situaciones especiales donde el Gerente o Subgerente considere necesario solicitar alguna restricción similar enviará la solicitud de igual manera.

Quien solicite un acceso a los sistemas de información de la empresa, deberá diligenciar todos los campos del FORMATO **DE REGISTRO DE AUTORIZACIONES (FOGI-04).**

8.2 Administración de Privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios en los Aplicativos deberán ser notificados al Área de Sistemas de Información, a excepción de los aplicativos netamente técnicos contratados y administrados por otra Área.

8.3 Equipo desatendido.

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el Área de Sistemas de Información cuando no se encuentren en su lugar de trabajo.

8.4 Administración y uso de Contraseña

La asignación de contraseñas debe ser realizada de forma individual, luego, el uso de contraseñas compartidas está prohibido.

Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Área de Sistemas de Información para que se le proporcione una nueva.

Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con la misma.

Todo usuario que sospeche que su contraseña es conocida por otra persona, deberá por precaución cambiarla inmediatamente.

El usuario deberá cambiar la contraseña inicial que se le asigne, en el primer acceso que realice al Sistema.

Se recomienda no incluir en la contraseña palabras, fechas o términos relacionados directamente con el empleado.

Las contraseñas deben ser actualizadas por los usuarios cada vez que lo consideren necesario y como mínimo una vez al año.

Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

La Gerencia General, la Subgerencia Administrativa y Financiera y el Área de Sistemas de Información, podrán bloquear el acceso si se sospecha que existe un riesgo en la seguridad del sistema o si tiene constancia del incumplimiento de las normas de seguridad.

8.5 Control de accesos remotos.

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Área de Sistemas de Información.

8.6 Política de Uso de Dispositivos de Almacenamiento Externos.

Está restringido el uso de dispositivos de almacenamiento externo como:

- Memoria Flash USB
- Reproductores portátiles MP3/MP4
- Cámaras con conexión USB
- IPhone/Smartphone
- SD Cards/Mini SD Cards/Micro SD Cards.
- PDAS/Tables
- Dispositivos con tecnología Bluetooth
- Tarjetas Compact Flash
- Discos duros de uso externo

8.7 Política de Navegacion en Internet.

Regular la navegacion por Internet a propósitos institucionales, educativos, de gobierno y demás páginas autorizadas por EMPAS S. A., de la siguiente manera:

- **Grupo Medio**: Este grupo solo navega a páginas institucionales, gubernamentales, educativas, Vanguardia Liberal, El Tiempo. NO TENDRÁ acceso a redes sociales, correo externo, youtube, dropbox o cualquier cloud o drive online, Canales Deportivos, Canal RCN, Canal Caracol, y no se puede hacer NINGUN TIPO DE DESCARGA.

  Para compartir información entre usuarios o dependencias se cuenta con el instructivo de manejo de carpetas compartidas, el cual el area de Sistemas de Informacion les indicara la forma de hacer uso de dichas carpetas.

  La hora feliz de 7:00 am a 8:00 am, donde podrá consultar correo externo (hotmail, Gmail, yahoo, etc.), diferentes periódicos, es decir navegación completa menos youtube ni redes sociales.

- **Grupo Alto**: Ademas de la navegacion del grupo Medio, tendrá navegación completa incluye youtube; y por definición no tiene acceso a las redes sociales.

- **Grupo Subgerentes**: Esta navegación incluye los dos grupos anteriores, mas redes sociales, youtube, restrigiendo la descarga de archivos .exe o ejecutables.

- **Grupo Elite**: Este grupo será exclusivo para usuarios que deben realizar descargas de software, por lo tanto el acceso es a todo nivel. (Sistemas).

La gerencia General, será la encargada de autorizar previa justificación la utilización de estos dispositivos y el acceso en cualquiera de los grupos de navegacion, para lo cual se requiere diligenciar el Formato de Registro de Autorizaciones - FOGI-04

9. SEGURIDAD DE COMUNICACIONES

La proliferación de software malicioso, como virus, spyware o programa espía, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí a través de la Red Interna de la Empresa y con terceros fuera de ella, por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

La empresa cuenta con contingencias en:

- Comunicación entre la sede de Alcantarillado y la Sede Administrativa con conexión en fibra óptica redundante.
- Se cuenta con un servidor de dominio de respaldo.
- Se cuenta con un servidor de aplicativos Windows de respaldo de la información.
- Se cuenta con un servidor de aplicativos web de respaldo de la información.
- Se cuenta con un servidor de copias de seguridad de respaldo.
- Servidor de Página web de respaldo

9.1 Topología de Red

El Área de Sistemas de Información deberá asegurar la integridad, disponibilidad y confidencialidad de los datos transmitidos, ya sea a través de dispositivos de hardware, de los protocolos de transmisión, o de los controles de aplicativos.

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

9.2 Conexiones Externas

El Área de Sistemas de Información deberá asegurar la implementación de elementos de control en las actividades de conexiones externas de EMPAS S.A a fin de garantizar la adecuada protección de los bienes de información de la organización.

9.3. Uso de Internet, Intranet y Correo Electrónico

a. El correo electrónico y el acceso a Internet constituyen parte de los medios puestos a disposición del personal para el adecuado desempeño de sus funciones, por lo que su utilización está exclusivamente encaminada a la ejecución propia de sus funciones.

b. La Intranet es un medio de comunicación interno y un sistema para la gestión de la información, que beneficia el trabajo de las personas por lo que se hace necesario darle un uso adecuado.

c. El acceso a Internet es completamente restringido y solo será autorizado a través del nivel directivo de la empresa, consultando siempre las necesidades de la función pública a desarrollar.

d. El administrador de la Red controlará el acceso a internet mediante una identificación del equipo en la red (dirección IP), administrada a través del Firewall

e. La cuenta de correo electrónico, propiedad de EMPAS S.A, está asignada a una persona para el desempeño de su función profesional. El usuario tiene acceso al correo electrónico suministrado por la empresa, durante el período de vigencia de su relación profesional con la misma, por lo que en el caso de que la relación se extinga o se suspenda, se interrumpirá el acceso a su buzón de correo electrónico.

f. El uso de correo institucional debe ser exclusivamente para temas laborales y no para recibir o enviar correos de contenido inadecuado y contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: preferencia de partidos políticos, apología del terrorismo, programas piratas, pornografía, amenazas, estafas, virus o código hostil en general, esquemas de enriquecimiento piramidal, cadenas de cartas y mensajes del tipo (renvía esta carta a 10 personas y tendrás una vida mejor) estos tres últimos son más conocidos como correo spam.

g. Es responsabilidad del usuario que descarga información directamente de internet ó a través del correo, vacunar inmediatamente esta información antes de ser abierta y/o distribuida, así mismo como abstenerse de abrir correos de dudosa procedencia y/o asunto sospechoso; debido a que puede estar siendo victima de spam, que son correos electrónicos masivos no solicitados, estos famosos spam amenazan la viabilidad del Internet como un medio efectivo de comunicación en la Empresa afectando los recursos de los servidores ya que al procesar spam hace lento el procesamiento del correo normal y otros procesos que tiene que ver con la productividad de la Empresa, puede dañar la infraestructura informática, por un uso inútil de la banda ancha, la denegación de servicio por saturación o la transmisión de virus y gusanos que afectarían la plataforma informática.

h. Es importante abstenerse también de dar información personal por la red, debido a que podemos estar siendo victimas de el famoso phishing que también es un tipo de spam cada vez más frecuente que conduce al robo de datos personales como números de tarjetas de crédito o contraseñas de bancos. Esto consiste, en envío de mensajes falsificados que parecen proceder de una organización seria y acreditada, como los bancos, empresas que ofrecen tarjetas de crédito o proveedores de servicios de Internet, se debe ser precavidos y asegurarse de que si van a brindar este tipo de información por este medio, realmente estén en la página verdadera del banco o entidad, usualmente estas entidades usan una mayor seguridad y verifican que sea el usuario el

que esta accediendo, y utilizan el protocolo ***https:// (protocolos seguro de transferencia de hipertexto).***

i. Los usuarios son los únicos responsables de todas las actividades realizadas con las cuentas de correo electrónico a ellos asignadas, por lo que deberán velar por el cumplimiento de las directrices y normas que se emitan en este sentido, se puede utilizar el instructivo para llevar a cabo el cambio de la contranseña para el correo Electronico (ITGI-03).

j. El servicio de navegación en Internet en la Empresa está sujeto al monitoreo de las actividades que realiza en Internet por parte del Área de Sistemas de Información.

k. Queda prohibido y se considerará como una falta grave:

1) El uso de internet en la oficina para fines personales toda vez que contraviene el Art. 60 del CST Numeral 8°: “Usar los útiles o herramientas suministradas por el empleador en objetos distintos del trabajo contratado” y lo establecido en la Ley 734/02 artículo 34 numeral 4 con las consecuencias establecido en dichas normas.

2) Toda transmisión o puesta a disposición de contenidos susceptibles de ser considerados delictivos, atentatorios contra la dignidad, el honor, la imagen o la intimidad de las personas o vulneradores de derechos de terceros, incluidos los de propiedad intelectual e industrial, así como cualesquiera otros inadecuados o no relacionados con el desempeño de las funciones propias del cargo.

3) Toda conexión remota desde el exterior de EMPAS S.A que no haya sido autorizada por el nivel directivo con observancia a los niveles de control respectivo, con la salvedad de los servicios corporativos que sean habilitados para su uso remoto. Esta autorización sólo se concederá cuando la función asignada al cargo lo requiera, y tras tener garantías suficientes de que no se verán afectados los niveles de seguridad de los sistemas de Información de la empresa.

4) La navegación por sitios con las siguientes características:
   - Alto contenido de gráficos, videos y fotografías (congestión en un alto porcentaje a la red).
   - Los archivos de música MP3 (ello constituye violación de los derechos de autor) y el respectivo almacenamiento de este tipo de archivos en los equipos de la Empresa.
   - Los sitios de contenido pornográfico, inmoral, ilegal, subversivo, sitios no deseados o de dudosa calidad y contenido.

5) Transmisión de archivos reservados o confidenciales no autorizados.

6) Descarga de software sin la autorización del Área de Sistemas de Información.

7) Descargar juegos a los equipos de la empresa o asignados a ésta.

l. A fin de garantizar la comunicación de los usuarios en General se permitirá el acceso a correos comerciales tales como Hotmail, Gmail, Yahoo entre otros, en el horario de 7:00 a 8:00 am y este horario será ampliado de acuerdo a la consideración del directivo inmediato. Esta directriz será aplicada a todos los funcionarios excepto el nivel directivo de la empresa.

m. El correo electrónico institucional todos@empas.gov.co disponible para enviar mensajes a todos los funcionarios de forma masiva debe ser utilizado únicamente para enviar información sobre temas laborales y su uso debe ser canalizado y autorizado por el Jefe de cada una de las Dependencias.

9.4 Antivirus

a. En todos los equipos de la empresa debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización del motor de detección no superior a una semana; toda información referente a virus se canalizará por el Área de Sistemas de Información para verificar su validez antes de darla a conocer a todo el personal.

b. Se prohíbe compartir en su totalidad el disco duro. De ser necesario compartir información, se debe crear una carpeta de sólo lectura en la cual se puede almacenar la información que es considerada temporal (Ver instructivo ITGI-05 para el uso de las carpetas compartidas) o hacer uso de la NUBE EMPAS (Ver instructivo ITGI-04 para utilizar la Nube en EMPAS) la cual deberá solicitarse al Área de Sistemas de Información previa autorización del Subgerente de cada dependencia, esto con el fin de prevenir la proliferación de virus informáticos en los Equipos de Cómputo de la institución.

c. La entidad contará con un FIREWALL (dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra). El firewall de la empresa debe presentar una postura de negación prestablecida, configurado de manera que se prohíban todos los protocolos y servicios que pongan en riesgo la seguridad de la información, habilitando los estrictamente necesarios.

10. SEGURIDAD DE LAS APLICACIONES

10.1. Software

a. El listado de software instalado en los equipos de cómputo será consultado a través de una Herramienta tecnológica seleccionada por el área de sistemas de información.

b. Los dueños de los Recursos Informáticos, que no sean propiedad de la entidad y quieran ser ingresados a la empresa para su utilización en la red, deben garantizar la legalidad del mismo,

demostrando que el software es gratuito o licenciado y que su uso es indispensable para el cumplimiento de sus funciones.

c. El grupo de soporte a usuarios adelantarán periódicamente revisiones para verificar el estado de licenciamiento de software de cada equipo al servicio de la empresa.

10.2. Seguridad de Bases de Datos

Los archivos indexados de la empresa, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deberán tener controles de acceso, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador de las Bases de Datos. Deberán hacerse chequeos regulares de la seguridad de la base de datos, para verificar que:

- Se hacen y son efectivos los backups y los mecanismos de seguridad
- No haya usuarios de la base de datos que no tengan asignado una contraseña
- Se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo.
- Nadie, además del administrador de datos, ha accedido a los archivos del software de base de datos y ha ejecutado un editor de archivos indexados.
- Solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa
- La base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.
- Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema. Los registros de la base de datos no se borrarán físicamente, sino que deberán marcarse como eliminados.

10.3. Control de Aplicaciones en PC’s

a. EMPAS S.A debe garantizar que los funcionarios usen programas de Computador de conformidad con las obligaciones de los tratados y la legislación Colombiana, en cumplimiento con la LEY 23 de 1982 sobre derechos de autor, por tanto la instalación de cualquier tipo de software en la empresa es función y responsabilidad exclusiva del Área de Sistemas de Información; cualquier otro software instalado sin autorización será responsabilidad del usuario. En caso de la detección de la instalación de un software sin el cumplimiento normativo

enunciado, el Área de Sistemas de Información de manera inmediata procederá a desinstalar y reportar esta situación al jefe inmediato.

b. El Área de Sistemas de Información será la encargada de realizar Mejoras y Ajustes a los sistemas de información cuando este sea solicitado por los usuarios, excepto las solicitudes de esta índole requeridas para los aplicativos técnicos contratados por las diferentes áreas de la empresa y sobre los cuales el Área de Sistemas de Información no tiene injerencia

c. Para la parametrización, alimentación y validación de las aplicaciones es necesario contar con el apoyo de los usuarios del sistema de información, esto solo para los Aplicativos que gestiona Sistemas de Información, con excepción de los aplicativos técnicos contratados por las diferentes áreas de la empresa. .

d. Cada responsable de cada proceso solicitará ante la Gerencia la necesidad de compra o implementación de nuevos programas para el desarrollo de sus actividades especificando sus requerimientos.

e. El Área de Sistemas de Información, evaluará la viabilidad de adquirir nuevos sistemas o aplicativos previa solicitud de las Dependencias y dará su concepto técnico para la toma oportuna de su decisión en caso de ser requerido por la Gerencia General y/o Subgerencias.

f. El nivel directivo es el competente y responsable de la solicitud y alcance de cada usuario de los sistemas de información. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud, en caso de rechazo el peticionario deberá acudir a la Gerencia como instancia definitiva.

g. El fondo de pantalla que deben tener los Equipos de Cómputo de EMPAS S.A, así como su protector de pantalla, debe corresponder al logo-Símbolo de la imagen institucional de la empresa, el cual será administrado por el Servidor de Dominio. El fondo de pantalla podrá ser cambiado para mostrar información relevante como políticas y recomendaciones de seguridad definidas en este manual.

h. Los accesos o perfiles de los usuarios tendrán la vigencia que se determine en el diligenciamiento del FOGI-04 FORMATO REGISTRO DE AUTORIZACIONES, en caso de darse una adición al contrato el Asesor, Subgerente o Gerencia General deberá remitir un correo electrónico al Área de Sistemas de Información indicando el nuevo plazo. Para el caso de personal de planta y una vez finalice su relación laboral con la empresa, se diligencia el FOGF-06 FORMATO PAZ Y SALVO, inmediatamente firmado se procede a la cancelación de la cuenta de red y correo electrónico.

10.4. Control de Datos en las Aplicaciones

El Área de Sistemas de Información:

- Aplicará controles para que los datos de entrada y salida del sistema sean verificables en su integridad, exactitud y validez.
- Restringirá con controles lógicos los datos de salida de los aplicativos de la empresa de acuerdo a los permisos de acceso.
- Establecerá medidas de identificación y autenticación para el acceso a dichos datos.

10.5. Backup

El Área de Sistemas de Información realizará copias de seguridad periódicas atendiendo a la criticidad de la información y se establecerá y cumplirá la política de realización de Backups de acuerdo al Plan de Copias de Seguridad de la Información, sujeto al procedimiento de esta actividad.

Para los sistemas de información que son gestionados y administrados por Dependencias del área técnica, es necesario que estas envíen comunicación formal al Asesor de Gerencia de Sistemas de Información con el fin de indicar cuales archivos se deben salvaguardar y su frecuencia de copiado. Cuando se requiera el acceso a un Backup deberá solicitarlo formalmente al Área de Sistemas. Cada vez que se produzca algún cambio deberá notificarse a Sistemas de Información para la reprogramación de la copia respectiva.

El Área de Sistemas de información no realizará la verificación de la generación correcta y restauración de los backups, esta responsabilidad será del área técnica correspondiente.

11. SEGURIDAD FÍSICA

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y Áreas restringidas de la EMPRESA sólo a personas autorizadas para salvaguardar los equipos de cómputo y comunicaciones de la empresa.

11.1. Control de Acceso Físico:

a. Cuando los usuarios se ausenten de sus estaciones de trabajo deberán cerrar todas las aplicaciones y documentos propios de su actividad a fin de prevenir que sus documentos o soportes de información sean sustraídos con facilidad, o que sean modificados o eliminados, así mismo deberán apagar íntegramente el equipo, incluyendo pantalla y CPU en cumplimiento a las medidas ambientales y de austeridad en el gasto.

b. Se restringe el acceso físico a las áreas críticas permitiéndose a los usuarios y responsables de los procesos a fin de controlar y minimizar el riesgo de accidentes y actividades fraudulentas.

c. Se deberán utilizar sistemas de monitoreo automáticos o manuales, que controlen el acceso constantemente.

d. El área del Centro de Procesamiento de Datos donde se encuentran los servidores, el switch central y demás equipamiento crítico solo debe tener permitido el acceso al personal del Área de Sistemas de Información, el ingreso de otro personal para actividades asociadas a los mantenimientos de Aires acondicionados, UPS, Verificación de inventarios, Arreglos locativos, etc., será autorizado por el área de Servicios Generales. Posteriormente los funcionarios de Sistemas de Información verificarán el estado del Centro de Procesamiento de Datos con el fin de evidenciar si se presentó algún daño o alteraciones en los Equipos.

e. Cada Subgerencia debe reportar al Área de Sistemas de Información, retiros, traslados del personal a la Empresa, puesto que es primordial tener actualizada la base de datos del sistema de atención al usuario, cuentas de correo y equipos de cómputo.

11.2. Control de Acceso a Equipos y Elementos de la Red de Datos

a. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la previa autorización del Área de Sistemas de Información, en caso de requerir este servicio deberá solicitarlo al Área de Sistemas de Información.

b. Los equipos de usuarios terceros o contratistas que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad.

c. La instalación, traslado y configuración de computadores, elementos de red, servidores, periféricos y en general cualquier equipo de cómputo que se integre a la red corporativa de la empresa será realizada únicamente por personal del Área de Sistemas de Información, previa autorización del Directivo Responsable de cada Proceso.

d. El Área de Sistemas de Información será la única encargada de llevar a cabo el encendido y apagado de los servidores que se utilizan en EMPAS S.A., siguiendo el instructivo para desarrollar esta actividad. (ITGI-02).

e. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

f. Los Usuarios deben evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU y mantener el equipo informático en un entorno limpio y sin humedad.

g. El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos.

h. Está prohibido que el usuario destape o desarme los equipos de cómputo.

i. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de EMPAS S.A, deberán ser notificados al Área de Sistemas de Información.

j. Los equipos de cómputo de la empresa deberán tener una contraseña de administrador para la configuración del sistema operativo, que deberá gestionar el administrador de la red.

k. Se prohíbe extraer de su ubicación cualquier elemento hardware, excepto aquellos que por su característica de portátil o móvil sean dedicados a aplicaciones de movilidad, tales como los computadores Portátiles.

l. El usuario será responsable de salvaguardar su información almacenada en su equipo. Como elemento de prevención para la pérdida de información, el usuario solicitará al asesor de su proceso la respectiva copia de la información, el Área de Sistemas de Información apoyará esta gestión de realizar la copia, y este backup realizado reposara con el asesor que realizó esta solicitud.

m. Los usuarios no podrán modificar las medidas técnicas de seguridad implantadas en los equipos de cómputo.

n. Únicamente el personal autorizado por el Asesor de Gerencia - Sistemas de Información podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

o. El usuario que tenga asignado algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

p. El usuario deberá dar aviso inmediato al Área de Sistemas de Información e Inventarios de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su custodia para su reposición, investigación y acciones administrativas y disciplinarias a lugar.

q. En el supuesto de que se produjera cualquier situación que pudiera poner en riesgo la seguridad de los sistemas de información de la empresa, el usuario deberá notificar la incidencia producida inmediatamente al Área de Sistemas de Información.

11.3 Dispositivos de Seguridad y Soporte

Los usuarios de EMPAS S.A que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser spam, phishing, espías, virus, caballos de Troya, gusanos de red entre otros.

Toda solicitud de instalación de software debidamente licenciado que no sea propiedad de EMPAS S.A, deberán justificar su uso y legalidad ante el Área de Sistemas de Información, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá este software.

Se considera una falta grave que los usuarios instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de EMPAS S.A, que no esté autorizado por el Área de Sistemas de Información.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de los Directivos competentes, el usuario informático deberá notificar esta situación al Subgerente respectivo.

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Área de Sistemas de Información, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de EMPAS S.A, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a EMPAS S.A, a menos que cuente con la autorización del Directivo correspondiente.

EMPAS S.A se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática de esta Empresa o realizado acciones no autorizadas.

El usuario debe tener claro que el correo electrónico de EMPAS S.A. es un correo de trabajo y No Personal, y se debe utilizar única y exclusivamente a los recursos que tenga asignados y las facultades que se le concedieron, para el desempeño de su empleo, cargo o comisión quedando prohibido cualquier otro uso.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

Los usuarios autorizados para el manejo de discos flexibles, CD's, DVD's, discos externos y USB, deben tener la cultura de verificar que la información y estos medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Área de Sistemas de Información.

Todos los archivos de computador que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Ningún usuario de EMPAS S.A debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computador diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computador, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de EMPAS S.A. El incumplimiento de este estándar será considerado una falta grave, debido a que estaría atentando contra la plataforma y red de nuestra entidad.

Cualquier usuario que sospeche de alguna infección por virus de computador, deberá dejar de usar inmediatamente el equipo y comunicar al Área de Sistemas de Información para la detección y erradicación del virus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por EMPAS S.A en: Antivirus, Outlook, Office, Navegadores u otros programas.

Los Usuarios deben velar por utilizar en forma debida las instalaciones eléctricas reguladas (REG.-1 – UPS2), abstenerse de conectar a ella equipos eléctricos diferentes a su equipo de computo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que sobrecargue los puntos, esto puede generar caídas de energía e incluso inconvenientes de mayor magnitud a la plataforma.

La Empresa debe suministrar los siguientes dispositivos de seguridad y soporte que garantizan la continuidad de los equipos:

- Aire acondicionado
- Extintores
- UPS: (Uninterruptible Power Supply)

- Descarga a tierra

Todos estos dispositivos de seguridad serán evaluados por personal de mantenimiento encargado por parte de la Subgerencia Administrativa y Financiera.

Como elemento de control se utilizará un tablero de distribución con sus respectivos interruptores de energía en la salida de emergencias de cada edificio.

12. NORMATIVIDAD APLICABLE

LEY 734/FEBRERO 2002 - CAPITULO SEGUNDO. - DEBERES.

ARTÍCULO34. - *DEBERES*. Son deberes de todo servidor público:

1. Cumplir y hacer que se cumplan los deberes contenidos en la Constitución, los tratados de Derecho Internacional Humanitario, los demás ratificados por el Congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y los manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas, los contratos de trabajo y las órdenes superiores emitidas por funcionario competente.

   Los deberes consignados en la Ley 190 de 1995 se integrarán a este código.

2. Cumplir con diligencia, eficiencia e imparcialidad el servicio que le sea encomendado y abstenerse de cualquier acto u omisión que cause la suspensión o perturbación injustificada de un servicio esencial, o que implique abuso indebido del cargo o función.

4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

7. Cumplir las disposiciones que sus superiores jerárquicos adopten en ejercicio de sus atribuciones, siempre que no sean contrarias a la Constitución Nacional y a las leyes vigentes, y atender los requerimientos y citaciones de las autoridades competentes.

11. Dedicar la totalidad del tiempo reglamentario de trabajo al desempeño de las funciones encomendadas, salvo las excepciones legales.

21. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.

22. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.

24. Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.

25. Poner en conocimiento del superior los hechos que puedan perjudicar el funcionamiento de la administración y proponer las iniciativas que estime útiles para el mejoramiento del servicio.

LEY 1273 DE 2009 DE DELITOS INFORMÁTICOS EN COLOMBIA

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
Dicha ley tipificó una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.
A continuación se mencionan los artículos que componen esta ley:

- **Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO**
- **Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.**
- **Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS**
- **Artículo 269D: DAÑO INFORMÁTICO**
- **Artículo 269E: USO DE SOFTWARE MALICIOSO**
- **Artículo 269F: VIOLACIÓN DE DATOS PERSONALES**
- **Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES**
- **Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES**

- **Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS**

13. TERMINOLOGÍA

Es una recopilación de palabras claves que se encuentran en el documento, las cuáles pueden ser términos técnicos, o bien palabras con un significado especial para el proceso definido. Su objetivo es lograr que se maneje un mismo concepto y evitar cualquier tipo de confusión para el correcto entendimiento del documento. Su estructura deberá ser por orden alfabético y la definición de los términos deberá ser clara y breve.

Se recomienda marcar en el documento con negritas o en cursiva las palabras claves que puedan causar mayor conflicto para el entendimiento general del proceso.

Acceso

Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.

Acceso Físico

Es la actividad de ingresar a una Oficina.

Acceso Lógico

Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo, o bien usar su información.

Acceso Remoto

Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de Coordinación amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.

Aplicación

Acción que se realiza a través de un programa de manera directa con el usuario. Navegadores, Chat, correo electrónico, etc. son algunos ejemplos de aplicaciones en el medio de Internet.

Antivirus

Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco duro o disquete.

Ataque

Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, por parte de un usuario no deseado ni autorizado a accederlo; con la finalidad de obtener acceso a ese activo y lograr afectarlo.

Archivo

Una colección identificada de registros relacionados.

Autorización

Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo a su perfil o puesto.

Base de Datos

Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

Brecha de seguridad

Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Cifrar

Quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama “descodificar” o “descifrar”. Los sistemas de cifra miento se llaman “sistemas criptográficos”.

Certificado Digital

Un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor

CD

Medio de almacenamiento de información.

Código Malicioso

Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.

Comprimir (Zip)

Reducir el tamaño de los archivos sin que éstos pierdan nada de su información. Zip es el nombre de la extensión que contiene un archivo comprimido.

Computador

Es un conjunto de dispositivos electrónicos que forman una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas.

Control de Acceso

Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.

Copyright

Derecho que tiene un autor, incluido el autor de un programa informático, sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida. El símbolo de este derecho es ©.

Correo Electrónico o E-mail

La funcionalidad es similar a usar el correo normal, pero ahora el individuo puede utilizar un computador y un software para enviar mensajes o paquetes a otro individuo o grupo de personas a una dirección especifica a través de la red o Internet.

Cuentas de Usuario

Es un identificador, el cual es asignado a un usuario del sistema para el acceso y uso del computador, sistemas, aplicaciones, red, etc.

DVD

Medio de almacenamiento de información.

Descargar

Acción de transferir información computarizada de un computador a otro.

Descomprimir (unzip)

Acción que se lleva a cabo después de haber comprimido un archivo para regresarlo a su estado original.

Discos flexibles (diskettes)

Medios de almacenamiento magnéticos de información de 1.44 MB llamados comúnmente discos de 3 ½.

Discos Ópticos

Los discos ópticos son medios de almacenamiento de información que presentan una capa interna protegida, donde se guardan los bits mediante el uso de un rayo láser, éste al ser reflejado, permite detectar variaciones microscópicas de propiedades “óptico-reflectivas” ocurridas como consecuencia de la grabación realizada en la escritura. Un sistema óptico con lentes encamina el haz luminoso, y lo enfoca como un punto en la capa del disco que almacena los datos.

Dominio

Sistema de denominación de host en Internet. Conjunto de caracteres que identifica y diferencian los diferentes sitios Web.

Encripción

Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encripción como tal, no existe en el lenguaje español, el término correcto es cifrado de datos.

Estándar

Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

Freeware (Software Libre)

Programas que se pueden bajar desde Internet sin cargo.

FTP

Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadores sobre un ambiente de red.

Gusano

Programa de computador que puede replicarse a sí mismo y enviar copias de un computador a otro a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

Hardware

Se refiere a las características técnicas y físicas de los computadores.

Help Desk

Soporte técnico brindado a los usuarios telefónicamente, su función es proveer conocimientos especializados de los sistemas de producción para identificar y asistir en el ámbito / desarrollo de sistemas y en la resolución de problemas.

Herramientas de seguridad

Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Empresa.

Impacto

Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza

Incidente de seguridad

Cualquier evento que represente un riesgo para la adecuada conservación de la confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función Información.

Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en Imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Internet o World Wide Web (www)

Es un sistema a nivel mundial de computadores conectados a una misma red, conocida como la red de redes en donde cualquier usuarios consulta información de otro computador conectado a esta red e incluso sin tener permisos necesarios acceder a dichos activos.

Intrusión

Es la acción de introducirse o acceder sin autorización a un activo tecnológico.

Lenguaje de Programación

Sistema de escritura para la descripción precisa de algoritmos o programas informáticos.

Maltrato, descuido o negligencia.

Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la EMPRESA.

Mecanismos de seguridad o de control

Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Medios Magnéticos (medios de almacenamiento)

Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (Diskettes, CDs, DVDs, Cintas, Cartuchos, etc.).

Metodología

Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente definidas.

Módem

Es un aparato electrónico que se adapta una Terminal o computador y se conecta a una red de comunicaciones (red telefónica). Los módems convierten los pulsos digitales de un computador en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

“Necesidad de saber”, principio o base

Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Empresa.

Nodo

Punto principal en el cual se les da acceso a una red a las terminales o computadores.

No repudio

Este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

Normatividad

Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización

Parche (patch)

Un parche (algunas veces llamado Fix) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la seguridad o incrementar la funcionalidad del mismo.

Password

Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a un computador personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6-10 caracteres alfanuméricos.

Phishing

Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Política

Son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático

Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Respaldo

Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo

Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.

Spam

Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Servidor

Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sitio Web

El sitio Web es un lugar virtual en el ambiente de Internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.

Spyware

Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Software

Programas y documentación de respaldo que permite y facilita el uso del computador. El software controla la operación del hardware.

Software Antivirus

Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de los computadores.

Software Malicioso

Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

Switch

Dispositivo de red que filtra y direcciona paquetes a las direcciones destinatarias. El switch opera en la capa de enlace de datos del modelo OSI.

Tarjeta Inteligente

Es una tarjeta de plástico del tamaño de una tarjeta de crédito, que incorpora un microchip, en el cual se puede cargar datos como números telefónicos anteriormente llamados, pagos realizados a través de medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.

Troyanos

Se denomina Troyano o Caballo de Troya a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Usuarios Terceros

Todas aquellas personas naturales o jurídicas, que no son funcionarios de EMPAS S.A, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos.

User-ID (identificación de usuario)

Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, números o signos.

Usuario

Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computador personal, o dispositivo (hardware).

Virus

Programas o códigos maliciosos diseñados para esparcirse y copiarse de un computador a otro por medio de los enlaces de telecomunicaciones o al compartir archivos o diskettes de computadores.

Vulnerabilidad

Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencionado o accidental.

ANEXOS

ANEXO 1. PROCEDIMIENTO DE GENERACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Este documento es relacionado con fines exclusivamente informativos y no será publicado ya que el contenido del mismo es de confidencialidad e importancia para el Área de Sistemas de Información.

ANEXO 2. PROCEDIMIENTO PARA LA INSTALACIÓN Y ACTUALIZACIÓN DEL ANTIVIRUS

Este documento es relacionado con fines exclusivamente informativos y no será publicado ya que el contenido del mismo es de confidencialidad e importancia para el Área de Sistemas de Información.

ANEXO 3. ESQUEMA DE UBICACIÓN DEL CENTRO DE CÓMPUTO

Dentro de la Sede Administrativa, en el piso 3 se encuentra ubicado el Centro de Cómputo.

Este sitio cuenta con:

- Un tablero de energía eléctrica, el cual tiene entradas y salidas de la corriente normal y corriente regulada.
- 2 UPS, una de 20 kva y la otra de 10 kva
- Cuenta con un rack de comunicaciones de voz y de datos.

- Un (1) sensor de temperatura y humedad.
- Un (1) rack, para organizar los servidores.
- 6 Servidores.
- Un archivador para almacenar las licencias del software utilizado en los diferentes equipos de computo.
- 2 Aires acondicionados, los cuales trabajan en forma alterna.
- 1 DVR para el Sistema de Cámaras de la Sede Administrativa

En el piso 3 de la sede de alcantarillado tenemos hay un centro de cómputo, el cual consta de lo siguiente:

- Un tablero eléctrico de distribución de corriente regulada y no regulada.
- 1 UPS de 20 kva.
- 1 Rack de comunicaciones.
- 2 aires acondicionados que trabajan de manera alterna.
- 1 Servidor
- 1 DVR para el Sistema de Cámaras de la Sede Alcantarillado

La conectividad entre las dos sedes (Administrativa y Alcantarillado) es en fibra óptica con canal redundante o backup.

DIAGRAMA DE RED DE EMPAS S.A