CÓDIGO: MAGI-01

VERSIÓN: 01

FECHA: 10/06/2021

MANUAL DE ADMINISTRACIÓN DE TECNOLOGIAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CUADRO CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del Cambio**
00	02/06/2021	Emisión inicial
01	10/06/2021	Cambio de nombre por Manual de tecnología, seguridad y privacidad de la información.

TABLA DE CONTENIDO

1. INTRODUCION

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. OBJETIVO GENERAL

Establecer directrices y lineamientos para la gestión de seguridad y privacidad de la información en la Empresa Pública de Alcantarillado de Santander S.A. E.S.P.

4. OBJETIVOS ESPECIFICOS

1. 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.

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

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

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

5. Establecer controles precisos 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.

6. 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.

5. ALCANCE

El manual consigna todas las políticas de gestión de seguridad y privacidad de la información de EMPAS S.A, para salvaguardar todos los activos de información y

que son de obligatorio cumplimiento por parte de los servidores públicos, contratistas, proveedores y colaboradores.

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. TERMINOLOGÍA

- **Activos de información:** elementos de hardware y software que permites la administración y funcionamiento de la información.
- **Clasificación de la información:** ejercicio en la que se determina el nivel de importancia de la información que se maneja en una entidad asegurándola y garantizándole una adecuada administración.
- **Confidencialidad:** La confidencialidad es la garantía de que la información personal o de una empresa será protegida para que no sea divulgada sin consentimiento.
- **Custodio técnico:** proceso o grupo de trabajo encargado de administrar y hacer efectivo los controles de seguridad de la información disponibles en la entidad.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y recursos asociados cuando se requiera.
- **Dominios de control:** guía que permite garantizar la seguridad de la información.
- **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.
- **Información:** activo esencial para las actividades de la entidad.

- **Integridad:** salvaguardar la información y sus métodos de procesamiento de forma exacta y completa
- **Propietario de la información:** designación de un propietario o grupos que tienen la responsabilidad de definir quienes tienen acceso a la información y que se debe hacer con esta.
- **Seguridad de la información:** Conjunto de políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.
- **Usuario:** Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la Entidad en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía.

7. AUTORIDAD Y RESPONSABILIDAD

7.1. COMPROMISOS DE LA GERENCIA

La gerencia de la Empresa Pública de Alcantarillado de Santander apoya de manera activa el establecimiento, mantenimiento y mejora continua de las políticas de seguridad de la información que se implementan en la entidad, a través de:

- Revisiones periódicas a las políticas de seguridad y privacidad de la información, así como el cumplimiento de estas.
- Asignación de recursos para gestión de la seguridad de la información.
- Promover la importancia de la seguridad de la información en la entidad para que los funcionarios de EMPAS obtengan una cultura organizacional de la seguridad y privacidad de la información.
- Apoyar el cumplimiento del Modelo de Seguridad y Privacidad de la Información definido por el MINTIC, las normas y estándares que lo complementen.

7.2. RESPONSABILIDAD

Es responsabilidad de la gerencia, subgerentes, asesores y jefes de oficina de la Empresa Pública de Alcantarillado de Santander hacer uso de las políticas de seguridad y privacidad de la información, como parte de sus herramientas de su gestión.

7.3. CUMPLIMIENTO Y VIOLACIONES

El cumplimiento de la política de seguridad y privacidad de la información se aplican a todos los servidores públicos, contratistas, proveedores y colaboradores que interactúan con los activos de información de la empresa o en calidad de responsables, custodio o usuarios. 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, Ley 1273 de 2009 Delitos Informáticos y la Ley 1581 de 2012 de Protección de Datos Art. 23 y 24.

ARTÍCULO 734. - 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.
3. 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.
4. 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.
5. 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.

6. Dedicar la totalidad del tiempo reglamentario de trabajo al desempeño de las funciones encomendadas, salvo las excepciones legales.
7. 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.
8. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.
9. Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.
10. 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**

7.4. APROBACIÓN Y ACTUALIZACIÓN DE LAS POLÍTICAS

Toda política de seguridad y privacidad de la información nueva, actualizada, y/o eliminada, será propuesta por el Área de Sistemas de Información y aprobada por el Comité Institucional de Gestión y Desempeño de EMPAS S.A. Estas políticas serán revisadas como mínimo una vez al año y/o cada vez que surjan cambios sustanciales o sean requeridos.

7.5. VIGENCIA DEL DOCUMENTO

Las políticas contenidas en este documento estarán vigentes desde la fecha de su aprobación.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. ORGANIZACIÓN INTERNA

8.1.1. Roles y Responsabilidades Para la Seguridad de la Información

Todos los funcionarios públicos, contratistas y terceros de EMPAS, deben conocer y cumplir el modelo de seguridad y privacidad de la información establecido en la empresa; la gestión de la seguridad y privacidad de la información incluye a todos los niveles organizacionales de la entidad, por lo que se asignan roles y responsabilidades para el cumplimiento de las políticas de seguridad y privacidad de la información.

I. Nivel Estratégico

Rol Comité Institucional de Gestión y Desempeño: asume la responsabilidad entorno a la planeación, ejecución, cumplimiento y mejora continua de las políticas de seguridad y privacidad de la información de EMPAS.

II. Nivel Operacional

Teniendo en cuenta que la Subgerencia de Planeación e Informática está integrado en este comité y ejerce la secretaria técnica, tiene la responsabilidad con el equipo interdisciplinario del Área de Sistemas de Información de garantizar el cumplimiento de las Políticas de Seguridad y privacidad de la información.

III. Nivel Comunidad

Todos los servidores públicos, contratistas y proveedores que pertenecen a EMPAS deben conocer y cumplir con las políticas de seguridad y privacidad de la información, salvaguardar los principios de seguridad de los activos de información, asistir a las capacitaciones y sensibilizaciones que programe la entidad en temas de seguridad de la información, aplicación y cumplimiento de controles para la protección de la información, identificación y clasificación de activos de información junto con un análisis de riego.

8.2. DISPOSITIVOS MOVILES Y TELETRABAJO

8.2.1. Políticas para Dispositivos Móviles

EMPAS S.A. debe controlar la seguridad de la información cuando se usan medios de computación móvil; para salvaguardar la información se debe:

- Estar autorizado para que los dispositivos móviles interactúen con la infraestructura para el procesamiento de la información de EMPAS S.A.
- Las personas autorizadas para el uso de dispositivos móviles que requiera tener acceso a la información desde redes externas podrán acceder remotamente mediante un proceso de autenticación.
- Concientizar a los funcionarios y contratistas sobre el riesgo de usarlos dispositivos móviles para manejar los sistemas de información como para la infraestructura tecnológica de la entidad.

8.2.2. Trabajo en Casa

La modalidad de trabajo en casa será posible para el personal vinculado a la entidad. Únicamente se asignarán conexiones a la red de EMPAS S.A. para trabajo en casa cuando sea solicitado por escrito por el área de Gestión Humana al área de Sistemas de Información, previa autorización de la Gerencia.

El área de sistemas de información se encargará de implementar los controles de seguridad físicos y tecnológicos para proteger la confidencialidad, integridad y disponibilidad de la información y socializar las medidas de seguridad y privacidad, las buenas prácticas para proteger la información. Los funcionarios que tengan conexión remota, no deben instalar ningún software en los equipos designados por la entidad.

9. SEGURIDAD EN EL RECURSO HUMANO

Todo el personal ya sea de planta o contratistas deben presentar al área de Sistemas de Información el formato FOGI-04 debidamente diligenciado para poder dar acceso al usuario y permisos de aplicativos en los cuales van a trabajar. Para el caso de los contratistas los accesos y perfiles tendrán vigencia hasta la fecha de caducidad del contrato, la cual debe ser diligenciada en el formato, y para el personal de planta se procede a realizar la cancelación de cuentas una vez finalice su relación laboral con la empresa, presentando el formato de paz y salvo FOGF-06 debidamente diligenciado.

10. GESTION DE ACTIVOS

EMPAS S.A. cuenta con una metodología, procedimiento, guía y formatos para identificar, clasificar y valorar los activos de información de todos los procesos al interior de la Entidad.

10.1. RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACIÓN

10.1.1. Inventario de Activos de Información

El inventario de los activos de información se hace con el fin de identificar cuáles son los más importantes para EMPAS S.A., para darle el tratamiento adecuado en el cumplimiento de los objetivos misionales y estratégicos de la Entidad

- Toda la información producida, gestionada y transmitida que hace uso de los recursos físicos y tecnológicos de EMPAS S.A. es de propiedad de la Entidad, a menos que se especifique lo contrario a través de un contrato u otro medio legal suscrito por el Representante legal de la Entidad. Por ello, el tratamiento de la información institucional está sujeto a lo establecido en las cláusulas de propiedad intelectual y confidencialidad incluidas en los contratos establecidos con los colaboradores y en los contenidos de este manual, con objeto de garantizar que no se realice uso de esta, con propósitos personales comerciales o de otra índole.

- Todos los funcionarios, contratistas y terceros deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de EMPAS S.A.

10.1.2. Propiedad de los Activos

La propiedad del activo se le debe asignar a un cargo, un proceso o grupo de trabajo que tendrá la responsabilidad de garantizar que la información y los activos asociados con los procesos se gestionen de manera adecuada. Por tal razón el propietario del activo de información en la entidad deberá:

- Asegurarse de que el activo asignado se encuentra en el inventario de EMPAS
- Asegurar que los activos estén clasificados y protegidos apropiadamente.
- Definir y revisar periódicamente las restricciones de acceso y las clasificaciones.

10.1.3. Uso aceptable de Activos

Todos los colaboradores a los que se le haya asignado activos de información para el desarrollo de sus funciones contractuales, deben cumplir los siguientes lineamientos:

- Toda actividad de administración y operación que se realice con los activos de información de propiedad de EMPAS S.A, deben estar orientadas única y exclusivamente a cumplir con los procesos misionales de la Entidad.

- Todos los colaboradores deben aplicar los controles de seguridad definidos en el presente manual, para reducir riesgos que afecten la integridad, confidencialidad y disponibilidad de los activos de información.

- Los activos de información que almacenen o usen datos personales sensibles, tendrán acceso controlado que será garantizado por el responsable de la custodia de la información.

- Ningún colaborador puede compartir sus credenciales de autenticación para acceder a los activos de información

- Cualquier modificación que se le deba hacer a los activos de información, debe ser autorizada por su propietario y verificada por el Área de Sistemas de Información

- Todos los colaboradores deben reportar al Área de Sistemas de Información cualquier evento que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información.

- Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

- Es responsabilidad de todos los funcionarios y contratistas de EMPAS S.A. reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los activos de información.

- No está permitido el uso de los recursos tecnológicos para difundir o participar en actividades publicitarias externas a EMPAS S.A.

Uso Aceptable equipos de cómputo

- A los colaboradores de EMPAS S.A. que para el cumplimiento de sus obligaciones requieran del uso de un equipo de cómputo, se les podrá asignar y entregar uno de escritorio o portátil, una vez legalizado su contrato o vinculación con la Entidad y diligenciado el formato FOGI-04.

- Una vez efectiva la entrega, los colaboradores son responsables por todos los elementos que se encuentren incorporados o hacen parte del equipo asignado (CPU, Teclado, Mouse, Pantalla, entre otros).

- La configuración, instalación, desinstalación y mantenimiento de hardware y software operativo, base, de aplicación y utilitario de los equipos de cómputo y de los dispositivos periféricos como impresoras o escáner, así como equipos de comunicaciones como Router, Switch y Access Point, son responsabilidad única del Área de Sistemas de Información de EMPAS S.A.

- Los colaboradores tienen prohibido instalar software no autorizado en los equipos de cómputo de la empresa.

Uso aceptable del correo corporativo

- Los colaboradores de EMPAS S.A. no deben emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Entidad, en especial, cuentas de correo personal.

- La responsabilidad del contenido de los mensajes de correo electrónico es del usuario remitente. En los procesos de reenvío de estos, no se deben alterar los datos originales.

- No está permitido crear, enviar, o retransmitir mensajes de correo electrónico que contengan contenido textual y/o gráfico que constituya acoso, que puedan contribuir a un ambiente de convivencia hostil, o que sean considerados difamatorios, explícitamente sexuales o que puedan ofender a alguien con base

en su raza, género, nacionalidad, orientación sexual, religiosa o política, apariencia física, estrato social o discapacidad.

- Está prohibida la generación, reproducción y envío de mensajes en cadenas o similares, debido a que esto puede habilitar la propagación de código malicioso (virus, troyanos, entre otros), saturar el tráfico de correo causando indisponibilidad del servicio o provocar fuga de información a través de mecanismos como spam, phishing, entre otros.

- El envío de mensajes a grupos de usuarios múltiples como “Todos o Contratistas” únicamente está habilitado para la Gerencia, Subgerentes, Jefes de Oficina y Asesores.

- Los mensajes de procedencia dudosa o desconocida no deben ser respondidos y deben ser clasificados por el usuario como correo no deseado. Lo anterior con el objeto de mitigar los riesgos relacionados con eventos de software malintencionado.

- A pesar de que las herramientas tecnológicas institucionales como el antivirus realizan un análisis de los archivos adjuntos de correo, para determinar si éstos contienen código malicioso, no se deben descargar archivos adjuntos de destinatarios desconocidos o sospechosos.

- El área de Sistemas de Información socializará con todo el personal las políticas de uso seguro del correo institucional.

- EMPAS S.A., con el objetivo de apoyar el desarrollo de las actividades institucionales, brinda acceso a Internet a sus colaboradores, con base en grupos de navegación definidos. Teniendo en cuenta que los recursos de la Entidad deben ser optimizados, los usuarios deben dar un uso racional al servicio de Internet y acoger los lineamientos en el Manual de Administración de Tecnologías de la Información – MAGI-01.

- La entidad se reserva el derecho de realizar revisiones periódicas al cumplimiento de los lineamientos definidos sobre el uso de Internet. y podrá aplicar restricciones o medidas en caso de que se encuentren excesos o la utilización indebida de ese recurso

- No está permitido el acceso a sitios pornográficos, con especial énfasis en los que involucran pornografía infantil, de contenido erótico, obsceno y sitios terroristas.

- La utilización de chat o mensajería instantánea, la descarga de música, radio o video en vivo es discrecional y está sujeta a la definición de perfiles de navegación que realice el área de sistemas de información. El acceso a sitios web que no se encuentren dentro de las categorías mencionadas en el MAGI-01, pero que requieran ser accedidas por los colaboradores para cumplir con sus obligaciones, podrán someterse a consideración de esta área, previa solicitud del Jefe de Área.

- Dado que la Entidad tiene la obligación legal de utilizar software licenciado, y que está comprometida con la protección de los derechos de propiedad intelectual y con la optimización del recurso de ancho de banda de las redes, los usuarios no deben descargar desde Internet, almacenar en la plataforma tecnológica de EMPAS S.A. y/o usar software, música, libros, publicaciones, video, entre otro material protegido por derechos de autor, sobre el cual la Entidad no haya realizado el pago de los derechos patrimoniales que corresponda.

- Los usuarios que utilicen Internet institucional para la realización de transacciones comerciales de carácter personal como pago de facturas, transacciones bancarias, entre otras, deben asumir los riesgos que dichas transacciones implican. EMPAS S.A. no se hace responsable de la seguridad de las mismas, incluyendo la información que se transmita y que pueda ser objeto del monitoreo que se realiza al uso de Internet.

- EMPAS S.A., con el objeto de dar cumplimiento a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Política de Gobierno Digital, dispone de cuentas en redes sociales, que se encuentran formalmente asignadas a unos responsables, por parte de la Oficina Asesora de Comunicaciones y que deben ser utilizadas bajo los protocolos de uso institucional, definidos para tal fin.

10.1.4. Devolución de Activos

- Todo activo de propiedad de la Entidad, asignado a un colaborador o a un tercero, deberá ser entregado al finalizar su vínculo contractual, por cambio de cargo o finalización de tareas específicas (terceros). Esto incluye los equipos de cómputo (Hardware y Software), dispositivos móviles, periféricos, manuales y la información que tenga almacenada en dispositivos móviles o removibles.

- Está prohibido el uso de equipos personales para las labores desempeñadas en la empresa, salvo autorización por parte de la Gerencia.

10.2. CLASIFICACIÓN DE LA INFORMACIÓN

10.2.1. Clasificación de la Información

- Toda la información existente generada en EMPAS S.A. debe ser clasificada por su responsable, con el objetivo de determinar controles específicos para su protección. La metodología para la clasificación de la información está armonizada con la Ley 1712 de 2014 o Ley de Transparencia y su aplicación será liderada por el Área de Archivo.

- EMPAS S.A. dispone de un inventario de activos de información y un Índice de Información Clasificada y Reservada, actualizados con periodicidad anual de acuerdo a lo establecido en la ley 1712 de 2014 acerca de la Transparencia y Acceso a la Información Pública.

10.3. MANEJO DE MEDIOS

10.3.1. Gestión de Medios Removibles

- No está permitido el uso y conexión de dispositivos de almacenamiento (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, celulares, cintas, etc.) sobre la infraestructura tecnológica de la empresa y únicamente se asignarán permisos a aquellos funcionarios cuyo perfil del cargo y funciones lo requiera, previa solicitud a través del formato FOGI-04 con visto bueno de Gerencia.

- Todo medio de almacenamiento removible debe ser sometido a análisis con la herramienta antivirus instalada en los equipos de EMPAS S.A.

- El Área de Sistemas de Información es responsable de implementar los controles necesarios para asegurar que únicamente los funcionarios autorizados, hagan uso de los medios removibles.

- Los medios de almacenamiento removibles que se conecten a los equipos de cómputo pueden estar sujetos a monitoreo por parte de Sistemas de Información, si se sospecha que incumplen las políticas descritas en este manual.

- EMPAS S.A. es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información, pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón quien haga uso de estos medios con la debida autorización, debe velar por la integridad y privacidad de la información contenida.

- No está permitida la ejecución de programas no autorizados desde algún medio extraíble identificado anteriormente.

11. CONTROL DE ACCESO

11.1. REQUISITOS DE EMPAS PARA EL CONTROL DE ACCESO

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.

11.1.1. Política de Control 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.

- No está permitido proporcionar información a personal externo, respecto a los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de EMPAS S.A.

- Cada persona que acceda a la infraestructura tecnológica de EMPAS S.A debe contar con un usuario único, el cual está compuesto por las tres primeras letras del nombre, las tres primeras letras del apellido y el número 01.

- Los usuarios son responsables de todas las actividades realizadas con su código de usuario.

- Los usuarios no deben divulgar ni permitir que otros utilicen sus credenciales de acceso a los sistemas de la empresa.

- El asesor del área de Gestión Humana notificará al correo de ayuda@empas.gov.co la novedad correspondiente cuando se trate de encargos, vacaciones o finalización de la vinculación, 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 que el área de Sistemas asigne a este los roles y permisos requeridos.

- En los casos de situaciones especiales donde el Gerente o Subgerente considere necesario solicitar alguna restricción debe enviar la solicitud al área de sistemas.

- 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).

11.1.2. Acceso a Redes y Servicios de Red

Internet

El grupo interno del área de sistemas de información regulará la navegación 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 y no se permite ningún tipo de descarga.

Para compartir información entre usuarios o dependencias se cuenta con el instructivo de manejo de carpetas compartidas, y se puede solicitar al área de Sistemas de Información.

Durante la hora feliz, de 7:00 am a 8:00 am, podrá consultar correo externo (Hotmail, Gmail, Yahoo, etc.), diferentes periódicos, es decir navegación completa con excepción de redes sociales.

- **Grupo Alto:** Además de la navegación 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, más redes sociales, YouTube, restringiendo 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.

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

- No está permitido el uso y conexión de dispositivos alternos, que provean servicio a internet y/o configurar los dispositivos de la entidad para el acceso a estos medios alternos.

- No se permite utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por Sistemas de Información.

Acceso Remoto

- Para el acceso y uso de VPN para conexiones remotas se requiere la solicitud del Jefe de Área. Será el área de sistemas quién asigne las conexiones remotas de acuerdo a las solicitudes enviadas al correo ayuda@empas.gov.co.

Carpetas compartidas

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.

11.2. GESTION DE ACCESO DE USUARIOS

- El Área de Sistemas de Información y los dueños de las aplicaciones deben revisar los derechos de acceso de los usuarios por lo menos una vez al año.

- El acceso a las plataformas, aplicaciones, servicios y en general a cualquier recurso de información de EMPAS S.A, debe contar con la autorización de las dependencias propietarias de los sistemas de información.

- Los privilegios de acceso se deben asignar a los usuarios, con base en las necesidades y eventos, sólo y durante el tiempo requerido y aprobado.

- No está permitido divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la contraseña de él(los) usuario(s) administrador(es) de la plataforma tecnología, dispositivos, bases de datos, equipos, servidores, aplicaciones, sistemas de información y similares.

- Toda asignación de permisos de acceso privilegiado debe contar con previa autorización del área de sistemas.

- Los derechos de acceso de todos los funcionarios, contratistas y terceros de acceso a la información y a los servicios de procesamiento de información se deben retirar al terminar su contratación laboral, contrato o acuerdo y/o se deben ajustar cuando existan cambios de dependencias y/o responsabilidades.

11.2.1. 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.

11.2.2. 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.

11.2.3. 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 seguro autorizado por el dueño de la información y del Área de Sistemas de Información.

El procedimiento para estos accesos es el siguiente:

a. El funcionario que requiera la conexión por vpn o acceso remoto, debe hacer la solicitud de través de su jefe de área, a través de un correo al área de sistemas, una vez recibido el correo, el asesor de sistemas se comunica con la gerente para la autorización de dicha vpn o acceso remoto.
b. Si la solicitud es aprobada, el área de sistemas asigna un numero de vpn y una contraseña de acceso al funcionario en el Firewall y se lleva una relación en una bitácora.

c. Se procede a contactar al funcionario para realizar la respectiva configuración en el pc de su propiedad. Esta conexión vpn solo está habilitada para ingresar a la intranet e interactuar con los diferentes aplicativos.
d. Si la conexión remota es autorizada, igualmente se realiza la configuración respectiva y se capacita al funcionario con respecto a la forma de establecer la conexión (conectar la vpn y luego escritorio remoto), además se le informa que el pc asignado en la empresa debe permanecer encendido y reiniciarlo, las veces que sea necesario (previo aviso del área de sistemas) para evitar bloqueos y permitir actualizaciones propias del sistema. Esta conexión remota permite al usuario trabajar con los documentos, archivos de su escritorio y correo Outlook como si estuviera ubicado frente al pc en la empresa.
e. Si la modalidad aprobada es la de trabajo en casa, el funcionario aporta el pc personal.
f. Cuando se requiere la modalidad de teletrabajo, este debe ser autorizado por la gerencia. Se debe solicitar el permiso a Servicios Generales para traslado del equipo de cómputo de las instalaciones de EMPAS a la residencia del funcionario.

11.2.4. Politices de Uso de Dispositivos de Almacenamientos Externos

Está restringido el uso de dispositivos de almacenamiento externo como:

a. Memoria Flash USB
b. Reproductores portátiles MP3/MP4
c. Cámaras con conexión USB
d. IPhone/Smartphone
e. SD Cards/Mini SD Cards/Micro SD Cards.
f. PDAS/Tables
g. Dispositivos con tecnología Bluetooth
h. Tarjetas Compact Flash
i. Discos duros de uso externo

11.3. RESPONSABILIDAD DE LOS USUARIOS

- Todos los funcionarios y contratistas, cuentan con un usuario y contraseña única, personal e intransferible y asumen su responsabilidad de los eventos e incidentes que puedan ocurrir bajo su autenticación sobre los activos de información a los cuales acceden y procesan dentro del desarrollo de sus funciones.

- Se debe dar uso adecuado a los activos de información y deben ser usados únicamente bajo las condiciones netamente laborales.

- Todos los funcionarios y contratistas, que requiera tener acceso a los sistemas de información de EMPAS S.A. deben estar debidamente autorizados y debe acceder a dichos sistemas haciendo uso de un usuario y contraseña.

- Construir contraseñas seguras que incluyan como mínimo: 1 carácter en Mayúscula, 1 carácter en Minúscula, 1 carácter numérico. Debe contener una longitud mínima de 8 Caracteres.

- 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 cada tres meses.

- 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.

11.4. CONTROL DE ACCESO A LOS SISTEMAS Y APLICATIVOS

El Área de Sistemas de Información, es la única dependencia que cuenta con la facultad para crear, asignar, bloquear, retirar y modificar, usuarios y permisos de acceso a los sistemas de la empresa.

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

12. SEGURIDAD FISICA Y DEL ENTORNO

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.

12.1. ÁREAS SEGURAS

- 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

- Se restringe el acceso físico a las áreas críticas (cuartos de servidores) a usuarios no permitidos y a fin de controlar y minimizar el riesgo de accidentes y actividades fraudulentas. Solo tiene 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.

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

- 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.

12.2. EQUIPOS

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos. En caso de requerir este servicio deberá solicitarlo al Área de Sistemas de Información.

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

- 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 realizado únicamente por personal del Área de Sistemas de Información, previa autorización del Directivo Responsable de cada Proceso.

- 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).

- El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información deben permanecer protegidos a través de canaleta para evitar el deterioro y garantizar la disponibilidad del servicio.

- 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.

- 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.

- Todos los equipos que contengan información sensible y/o confidencial en sus medios de almacenamiento deben pasar por un procedimiento de borrado seguro antes de su reutilización o finalización de su vida útil.

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

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

- 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 solicitados al Área de Sistemas de Información.

- 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.

- 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.

- El usuario será responsable de salvaguardar su información almacenada en su equipo.

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

- Únicamente el personal autorizado por el Asesor de Gerencia - Sistemas de Información podrá llevar a cabo los servicios y reparaciones al equipo informático.

- El usuario deberá dar aviso inmediato al Área de Sistemas de Información y Servicios Generales 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.

- 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

- 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 cómputo, 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:

  a. Aire acondicionado
  b. Extintores
  c. UPS: (Uninterruptible Power Supply)
  d. 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.

13. SEGURIDAD DE LAS OPERACIONES

13.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Es responsabilidad del Área de Sistemas de Información separar los ambientes de desarrollo, pruebas y producción de los desarrollos internos y externos.

13.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- En todos los equipos de la empresa debe existir una herramienta antivirus ejecutándose permanentemente.

- Se prohíbe compartir en su totalidad el disco duro. De ser necesario compartir información, se debe crear una carpeta compartida 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.

- La entidad cuenta con un FIREWALL (dispositivo que funciona como cortafuegos, permitiendo o denegando las transmisiones de una red a otra). El firewall de la empresa debe configurarse de manera que se prohíban todos los protocolos y servicios que pongan en riesgo la seguridad de la información, habilitando los estrictamente necesarios.

- 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.

13.3. COPIAS DE RESPALDO

- 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.

- 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.

- En caso de requerirse la inclusión de información adicional en el Plan de Copias de Seguridad, el jefe de área debe solicitarlo por escrito al área de sistemas de información.

- 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. Las copias manuales realizadas serán registradas en el formato FOGI-03 – Formato de registro de copias de seguridad y serán revisadas por el asesor de gerencia de sistemas de información

13.4. REGISTRO Y SEGUIMIENTO

- Se debe conservar un registro de todos los códigos fuente y las librerías de los aplicativos propiedad de EMPAS S.A. con el fin de facilitar las labores de revisión.

- Todos los relojes de los sistemas de procesamiento de información de EMPAS S.A. deben estar sincronizados con una fuente de tiempo exacto acordado.

- 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:

a. Se hacen y son efectivos los Backups y los mecanismos de seguridad

b. No haya usuarios de la base de datos que no tengan asignado una contraseña

c. Se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo.

d. 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.

e. Solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa.

f. La base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.

g. 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.

13.5. CONTROL DE SOFTWARE OPERACIONAL

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

- 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.

- 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.

- 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.

- 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.

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

- Los accesos o perfiles de los usuarios tendrán la vigencia que se determine en el diligenciamiento del FOGI-04 FORMATO REGISTRO DE

AUTORIZACIONES. Para el caso de personal de planta y una vez finalice su relación laboral con la empresa, se debe diligenciar el FOGF-06 FORMATO PAZ Y SALVO, inmediatamente firmado se procede a la cancelación de la cuenta de red y correo electrónico.

13.6. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- Se deben realizar análisis de vulnerabilidades y riesgos para actualizar la matriz de riesgos del proceso de Gestión Informática.

- No está permitido que los funcionarios, contratistas y terceros realicen pruebas y/o aprovechen las debilidades de seguridad en la infraestructura tecnológica.

- Se debe restringir la práctica de instalación de software no autorizado a través de políticas de dominio y otorgar los permisos únicamente a los funcionarios autorizados.

14. SEGURIDAD DE LAS COMUNICACIONES

14.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

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.

14.1.1. 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.

14.1.2. 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.

14.1.3. Uso de Internet e Intranet

a. 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.

b. 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.

c. 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

d. Es responsabilidad del usuario que descarga información directamente de internet o 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 víctima 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.

e. Es importante abstenerse también de dar información personal por la red, debido a que podemos estar siendo víctimas del 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 está accediendo, y utilizan el protocolo https:// (protocolos seguros de transferencia de hipertexto).

f. 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.

g. 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.

h. 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.

14.2. TRANSFERENCIA DE INFORMACION

El intercambio de información entre empleados, contratistas y las diferentes áreas por medio electrónico debe ser realizado a través de correo institucional, carpeta compartida o Nube de la empresa.

Si la transferencia es a través del correo institucional la información enviada deberá incluir la respectiva firma del remitente y en su pie de página el siguiente aviso:

"LA EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P – EMPAS S.A. dando cumplimiento a lo estipulado en la Ley 1581 de 2012 y su decreto reglamentario 1074 de 2015, tendiente a la protección de datos personales lo invita a que conozca la Política de Tratamiento de Datos Personales la cual puede ser consultada en las instalaciones físicas de la entidad o en el sitio web www.empas.gov.co. En dicha política se establecen los derechos que le asisten como titular, el procedimiento para ejercerlos, las finalidades para la cual se tratan los datos, entre otros aspectos. Si usted tiene alguna inquietud frente al manejo de la información, envíe su solicitud a través de nuestra página web o al correo contactenos@empas.gov.co y con gusto será atendido."

Mensajería electrónica

- 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.

- 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.

- 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, esquemas de enriquecimiento piramidal, cadenas y en general, lo que se pueda considerar como correo spam.

- Es responsabilidad del usuario que descarga información directamente de internet o a través del correo, verificar con el antivirus esta información antes de ser abierta y/o distribuida, así mismo, abstenerse de abrir correos de dudosa procedencia y/o asunto sospechoso.

- 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 recomienda cambiar periódicamente la contraseña, siguiendo las indicaciones contenidas en el instructivo ITGI-03.

- Las listas de correo electrónico institucional (todos@empas.gov.co y contratistas@empas.gov.co) disponibles para enviar mensajes a todos los funcionarios y contratistas 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.

15. REFERENCIAS

- Guía 8 - Controles de Seguridad de la Información MINTIC
- NTC-ISO/IEC 27001
- NTC-ISO/IEC 27002
- Modelo Integrado de Planeación y Gestión, MIPG.
- Manual de Administración de Tecnología de la Información – MAGI-01

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 cómputo.
- 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 se cuenta con 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