Municipio de Quito

RESOLUCIÓN N° GG-2023-050

Ing. Othón Zevallos Moreno
GERENTE GENERAL
EMPRESA PÚBLICA METROPOLITANA DE AGUA POTABLE Y SANEAMIENTO

CONSIDERANDO:

Que, el artículo 82 de la Constitución de la República del Ecuador (en adelante la Constitución) dispone que: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes";*

Que, el artículo 226 de la citada Norma Suprema determina que: "*Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución*";

Que, el artículo 227 de la Constitución de establece que: "*La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación*";

Que, la Constitución, en la parte pertinente de su artículo 315, determina que el Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas. Las empresas públicas estarán bajo la regulación y el control específico de los organismos pertinentes, de acuerdo con la ley; funcionarán como sociedades de derecho público, con personalidad jurídica, autonomía financiera, económica, administrativa y de gestión, con altos parámetros de calidad y criterios empresariales, económicos, sociales y ambientales;

Que, el artículo 4 de la Ley Orgánica de Empresas Públicas (en adelante "LOEP"), establece que las empresas públicas, como entidades que pertenecen al Estado, son personas jurídicas de Derecho público, con patrimonio propio, dotadas de autonomía presupuestaria, financiera, económica, administrativa y de gestión, destinadas a la prestación de servicios públicos, entre otros; precisando además el numeral 4 del artículo 3 de la Ley Ibidem, que las empresas públicas se rigen, entre otros, por los principios de eficiencia, calidad y seguridad;

Que, el artículo 11 numerales 4 y 8 de la LOEP, prevé como atribuciones del Gerente General, las siguientes: *"(…) Administrar la empresa pública, velar por su eficiencia empresarial e informar al Directorio trimestralmente o cuando sea solicitado por éste, sobre los resultados de la gestión de aplicación de las políticas y de los resultados de los planes, proyectos y presupuestos, en ejecución o ya ejecutados (…) Aprobar y modificar los reglamentos internos que requiera la empresa, excepto el señalado en el numeral 8 del artículo 9 de esta Ley (…)";*

Que, el artículo 130 del Código Orgánico Administrativo (en adelante "COA"), determina que las máximas autoridades administrativas tienen competencia normativa de carácter administrativa para regular los asuntos internos del órgano a su cargo y los asuntos que la ley así lo determine;

Que, el literal e) del artículo 77 de la Ley Orgánica de la Contraloría General del Estado, determina que las máximas autoridades de las instituciones del Estado, son responsables de los actos emanados de su autoridad, y entre las atribuciones y obligaciones específicas está la de: *"(…) e) Dictar los correspondientes reglamentos y demás normas secundarias necesarias para el eficiente, efectivo y económico funcionamiento de sus instituciones (…)";*

Que, el artículo 188 del Código Municipal para el Distrito Metropolitano de Quito, crea la Empresa Pública Metropolitana de Agua Potable y Saneamiento (en adelante "EPMAPS");

Que, la EPMAPS de conformidad con lo dispuesto en los artículos 136 y 189 del Código Municipal para el Distrito Metropolitano de Quito, es una persona jurídica de Derecho Público, con patrimonio propio, dotada de autonomía presupuestaria, financiera, económica, administrativa y de gestión; creada con el objeto principal de diseñar, planificar, construir, mantener, operar y, en general, explotar la infraestructura de los sistemas para la captación, conducción, producción, distribución y comercialización de agua potable, la recolección y conducción de aguas lluvias; y, la recolección, conducción y tratamiento de aguas servidas; y, aprovechar los recursos hídricos como la utilización de la energía potencial almacenada en los embalses y caídas de agua para generación de electricidad, entre otros;

Que, las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos publicadas en el Primer Suplemento del Registro Oficial No. 257, de 27 de febrero de 2023; establecen disposiciones sobre la Seguridad de tecnología de información, protección de datos personales, propiedad intelectual del software, seguridad de la información y utilización de estándares que deben ser considerados en el desarrollo de las actividades empresariales;

Que, mediante Resolución No. 086 de 06 de julio de 2017, la Gerencia General expidió la Política Interna General de Seguridad de la Información y sus lineamientos, así como las Políticas Internas Específicas de Seguridad de la Información; y,

Que, a través del memorando No. GP-2023-181, de 21 de abril de 2023, la magíster Verónica Sánchez, Gerente de Planificación y Desarrollo, solicita a la Gerencia Jurídica que: *"(…) luego de la revisión de las Políticas Internas General y Específicas de Seguridad de la Información actualizadas por el Departamento Seguridad de la Información (…) remitió con memorando N° GP-2023-135 a los Gerentes miembros del Comité para la validación, obteniendo respuesta de la Gerencia Financiera mediante correo electrónico del 11 de abril de 2023 en el cual indicó que no existen observaciones a las Políticas. (…) se puso a consideración de la Dirección de Comunicación Social y Transparencia (…) teniendo respuesta con memorando N° EPMAPS-DC-2023-088 de 4 de abril de 2023, en el que solicitó la exclusión del literal g) por considerarlo innecesario y que no aborda competencias para esa Dirección; petición que ha sido recogida favorablemente (…) En vista de no haberse recibido observaciones adicionales, se procede a solicitar muy comedidamente la gestión pertinente para la aprobación por parte de la Gerencia General mediante Resolución, para lo cual se adjuntan el consolidado de Políticas Internas General y Específicas de Seguridad de la Información; así como el glosario de términos respectivo"; y,*

En ejercicio de las atribuciones conferidas por los artículos: 11 numerales 1, 2, 4, 8 y 18 de la Ley Orgánica de Empresas Públicas; 155, letras: a), b) y l) del Código Municipal para el Distrito Metropolitano de Quito; y, las letras a), e) y j) del artículo 12 del Reglamento Orgánico Funcional de la Empresa, Nivel Jerárquico Superior.

RESUELVE:

Art. 1.- Derogar la Resolución No. 086, de 06 de julio de 2017, a través de la cual se expidió la Política Interna General de Seguridad de la Información y sus lineamientos, así como las Políticas Internas Específicas de Seguridad de la Información.

Art. 2.- Aprobar y expedir la Política Interna General de Seguridad de la Información de la Empresa Pública Metropolitana de Agua Potable y Saneamiento y sus lineamientos, así como las Políticas Internas Específicas de Seguridad de la Información; mismas que constan en documentos anexos y que forman parte integrante de la presente resolución.

Art. 3.- Encárguese a la Gerencia de Planificación y Desarrollo a través del servidor designado como Oficial de Seguridad de la Información, la difusión, y ejecución de la presente Resolución en coordinación con las Gerencias de área y Direcciones de la Empresa de acuerdo al ámbito de su competencia.

Art. 4.- Delegar a la Gerencia de Planificación y Desarrollo la revisión y aprobación de documentos y procedimientos del Sistema de Gestión de Seguridad de la Información, siempre que éstos no impliquen responsabilidad intergerencial, en cuyo caso la revisión y aprobación estará a cargo del Comité de Investigación, Desarrollo, Innovación y Seguridad de la Información.

Municipio de Quito

Art. 5.- La presente Resolución entrará en vigencia a partir de su suscripción y deberá publicarse en la intranet y en la página web institucional.

Dado en el Distrito Metropolitano de Quito, el 11 de mayo de 2023.

Firmado electrónicamente por:
HUGO OTHON ZEVALLOS MORENO

Ing. Othón Zevallos Moreno
GERENTE GENERAL

Acción	Responsables	Siglas Unidades	sumilla
Elaborado por:	K. Parra	GJL	Firmado electrónicamente por: KEVIN FELIPE PARRA TOBAR Razón: Localización: Fecha: 2023-05-11T13:18:22.14051-05:00
Revisado y aprobado por:	V. Sánchez	GP	Firmado electrónicamente por: TERESA VERONICA SANCHEZ HIDALGO Razón: Localización: Fecha: 2023-05-11T13:35:14.776412-05:00
	P. Rojas	GJL	Firmado electrónicamente por: PIEDAD CATALINA ROJAS POLANCO Razón: Localización: Fecha: 2023-05-11T13:20:01.09764-05:00
	I Ubidia	GJ	Firmado electrónicamente por: IVAN FRANCISCO UBIDIA DONOSO Razón: Localización: Fecha: 2023-05-11T15:02:17.918227-05:00
Aprobado por:	C. González	GJ	Firmado electrónicamente por: ANGELA CRISTINA GONZALEZ CAMACHO Razón: Localización: Fecha: 2023-05-11T15:31:47.036307-05:00

POLÍTICAS INTERNAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

MSGSI-PG-A05.1-02 rev01

Para el cumplimiento de la Política Interna General de Seguridad de la Información, se describen a continuación las Políticas Internas Específicas encaminadas a la gestión de la confidencialidad, integridad y disponibilidad de la información Empresarial.

Estas Políticas son de aplicación obligatoria para todos los servidores de acuerdo a sus ámbitos de competencia; así como para terceros a quienes se les trasmita o tengan acceso a información institucional.

Estas políticas serán actualizadas por el servidor designado como Oficial de Seguridad de la Información, revisadas por el Gerente de Planificación y Desarrollo previa la validación del Comité de Investigación, Desarrollo, Innovación y Seguridad de la Información y puestas a consideración del Gerente General para su aprobación, cada dos años o cuando sea necesario.

I.- Políticas Internas Específicas de Seguridad de la Información: De Aplicación General

1.- Seguridad de la información en Teletrabajo
2.- Validación de antecedentes previa la contratación
3.- Inventario y clasificación de información
4.- Uso aceptable de activos de información
5.- Control de accesos lógicos (servicios y sistemas informáticos)
6.- Inicios de sesión seguros y gestión de contraseñas
7.- Control de acceso al código fuente
8.- Seguridad física y ambiental
9.- Seguridad de los equipos
10.- Escritorios y pantallas limpias
11.- Seguridad de la información en la relación con los proveedores y otros terceros
12.- Privacidad y protección de datos personales
13.- Propiedad Intelectual
14.- Prevención de fuga de información
15.- Gestión de incidentes de Seguridad de la información
16.- Seguridad de la Información en la Continuidad del negocio

II.- Políticas Internas Específicas de Seguridad de la Información: De Aplicación para la Gerencia de Tecnología de Información

1.- Gestión de cambios en la infraestructura, servicios y sistemas informáticos
2.- Protección contra código malicioso
3.- Respaldos de información
4.- Sincronización de registros
5.- Ambientes de desarrollo, pruebas y producción
6.- Desarrollo de Software
7.- Gestión de Portales Web
8.- Lineamientos para Sistemas de Información Geográfica

Para un mejor entendimiento de éstas políticas, se adjunta el Anexo de Glosario de Términos.

I.- Políticas Internas Específicas de Seguridad de la Información: De Aplicación General

1.- Seguridad de la Información en Teletrabajo

a) Los teletrabajadores serán responsables por el cuidado y custodia de los equipos informáticos, dispositivos móviles u otros activos de información empresariales que empleen para el desarrollo del teletrabajo.

b) Los teletrabajadores serán responsables de mantener la confidencialidad e integridad de la información que disponen, gestionan y está bajo su custodia para el desempeño de funciones.

2.- Validación de antecedentes previa la contratación

La Gerencia de Talento Humano, siguiendo la normativa legal vigente y en consideración del Reglamento Interno de Administración del Talento Humano (RIATH) y Reglamento Interno de Trabajo (RIT), previa la contratación de un servidor realizará las validaciones pertinentes de antecedentes de: Cumplimiento de competencias para el cargo, títulos académicos, experiencias anteriores y demás documentos requeridos previa la asignación del cargo de forma que la información empresarial que manejen los nuevos servidores sea protegida y aporten a su confidencialidad, integridad y disponibilidad según corresponda.

3.- Inventario y Clasificación de información

a) Los responsables de los procesos empresariales y/o Dueños de Datos (que corresponderán a los cargos de jefaturas de Unidades, Departamentos, Gerencias o Direcciones que se han identificado y según consten en el "Listado de Dueños de Datos" y "Matrices de Clasificación de Información" que se emitan en el Sistema de Seguridad de la Información), en coordinación con el Departamento Seguridad de la Información realizarán el inventario y clasificación de información conforme la planificación anual, de forma que la información esencial esté claramente identificada y clasificada de acuerdo a: Los requerimientos legales, valor, criticidad y sensibilidad ante su divulgación y modificación no autorizada.

b) El inventario y clasificación de información se revisarán cada dos años o cuando se produzcan cambios importantes en los procesos, por lo que los Dueños de Datos los reportarán al Departamento Seguridad de la Información para la actualización que corresponda.

4.- Uso aceptable de activos de información

a) Los servidores de la Empresa deberán ser capacitados de acuerdo a la planificación anual sobre los lineamientos o procedimientos de seguridad para el manejo de información; siendo su responsabilidad estar en conocimiento de los mismos, completar documentadamente las capacitaciones y aplicarlas en el desempeño de sus funciones.

b) Todos los servidores de la Empresa que hayan sido autorizados para tener acceso a información y a servicios informáticos:

i. Deberán hacer un buen uso de éstos y no ser usados para beneficio propio, ejecución de prácticas ilícitas o mal intencionadas o cualquier otra que atenten contra otros servidores, la Empresa, terceros, la legislación vigente o los lineamientos de Seguridad de la Información.
ii. Deberán cumplir con el Procedimiento de Entrega de Información que se establezca en el Sistema de Seguridad de la Información, siendo las Jefaturas inmediatas responsables de velar por el cumplimiento del mismo previo para la firma del formulario de liquidación por separación de la Empresa o por de movimientos de personal.
iii. Pondrán en conocimiento el presente lineamiento para su cumplimiento a terceros autorizados que interactúen con información empresarial.

5.- Control de accesos lógicos (servicios y sistemas informáticos)

a) Todos los servidores deberán tener un identificador de usuario único asignado y una contraseña personal secreta para acceder a los servicios informáticos de la Empresa.

b) Todas las acciones realizadas en un servicio informático serán imputables exclusivamente al servidor responsable por el identificador de usuario.

c) La solicitud de acceso a información empresarial deberá ser validada por el Jefe inmediato y autorizada por el Dueño de Datos de dicha información. Así mismo, los privilegios de accesos deberán habilitarse de acuerdo con la necesidad para el desempeño de funciones y conforme los perfiles de accesos autorizados según corresponda.

d) Los datos en producción podrán ser modificados por usuarios desarrolladores, administradores y de mantenimiento de los sistemas informáticos, únicamente en los siguientes casos debidamente autorizados por el Dueño de Datos:

i. Cuando se justifique técnicamente que no se dispone de un ambiente de desarrollo y pruebas.
ii. Cuando se justifique tecnológicamente que el aplicativo no dispone y no es factible poner a disposición de los usuarios finales funcionalidades adicionales que permitan el cambio o eliminación

de datos en ambientes productivos.

iii. Cambios o ingresos masivos o específicos debidamente justificados y documentados.
iv. Cuando se requiera ejecutar pruebas de error para la solución de problemas que no puedan ser replicados en ambientes de pruebas; siempre que se disponga de la autorización adicional del administrador del contrato según aplique.

e) Los responsables de los procesos y Dueños de Datos son quienes deberán validar la integridad de los datos que se gestionan en los servicios informáticos empresariales.

f) Los permisos para el control de acceso a información almacenada en equipos informáticos empresariales en carpetas compartidas de red, se deberán otorgar únicamente a los usuarios autorizados y con los perfiles pertinentes.

g) Los accesos en ambientes productivos de los servicios informáticos deberán contar con registros de auditoría; así como, también los cambios de datos y otras acciones según la definición de los Dueños de Datos, que permitan su trazabilidad para revisión de: Auditores internos o externos, servidor designado como Oficial de Seguridad de la Información, Dueños de Datos, Jefes inmediatos, etc. según corresponda.

h) Todo servicio informático que permita acceder y manejar de información que no sea de acceso público, deberá utilizar un sistema de control de accesos basado en perfiles o roles y cumplir los lineamientos respecto a gestión de contraseñas.

i) El uso de identificadores de usuarios genéricos y su gestión se limitará exclusivamente al Procedimiento para su creación y utilización vigente.

j) Todos los servicios informáticos de la Empresa, deberán estar configurados para permitir sólo tres intentos de introducir la contraseña correcta, luego de lo cual el identificador de usuario deberá quedar bloqueado, pudiendo reiniciarse según los procedimientos que se establezcan al respecto.

k) Todas las plataformas tecnológicas y servicios informáticos administrados por Tecnología de Información directamente o mediante un tercero, deberá contar con identificadores de usuarios principales para la administración y monitoreo de acuerdo a sus competencias; las claves de acceso de estos usuarios se dispondrán en sobre cerrado y con las seguridades del caso para situaciones de emergencia, bajo custodia de las jefaturas Departamentales.

l) Los administradores del servicio de internet empresarial tendrán en cuenta que terceros autorizados podrán ingresar únicamente al segmento de red para invitados; así mismo, cuando se autoricen permisos especiales de internet y que permitan de forma temporal o definitiva el acceso a plataformas externas para colocación de información, aplicará la habilitación del monitoreo del servicio de protección de información empresarial.

m) En caso de proveedores o terceros autorizados que dan soporte y/o servicios a la Empresa y que para sus actividades requieren acceder a los servicios informáticos utilizando la red corporativa empresarial se les asignará un identificador de usuario personal con los accesos requeridos previa validación que corresponda y autorización del Dueños de Datos.

n) Todo identificador de usuario establecido para un tercero autorizado deberá tener una fecha de vencimiento especificada, con vencimiento predeterminado de 30 días cuando no se conozca su vencimiento.

o) Cuando un servidor se separe de la Empresa, se deberán retirar todos los accesos que disponga y luego los identificadores de usuario deberán ser deshabilitados. Este lineamiento deberá aplicarse también para terceros autorizados al concluir sus actividades, pasantías o la relación vía contrato o convenio con la Empresa.

p) La Empresa se reserva el derecho de monitorear, bloquear, ocultar, negar o descontinuar sus servicios informáticos en cualquier momento y sin previo aviso a los servidores de la Empresa, basado en el justificativo técnico y/o administrativo que corresponda y que se relacione con la afectación a la Seguridad de la información empresarial.

q) Los permisos de accesos de los servidores, deberán ser evaluados al menos una vez al año y

determinar si dichos accesos siguen siendo requeridos para que los servidores puedan realizar sus actividades de acuerdo a sus funciones.

r) Los usuarios finales no podrán cambiar configuraciones a nivel de sistema operativo de los computadores asignados, salvo en los casos en los que técnicamente se justifique que el usuario final cambie la configuración regional del equipo.

6.- Inicios de sesión seguros y Gestión de contraseñas

a) El acceso a los servicios informáticos empresariales deberá ser controlado por un inicio de sesión seguro, se deberán limitar el número de intentos fallidos de conexión, cerrar las sesiones luego de transcurrido un tiempo de inactividad y no mostrarán las contraseñas que ingresan los usuarios en texto claro.

b) Las contraseñas deberán tener una longitud mínima de 8 caracteres, usando una combinación de letras mayúsculas, minúsculas, números y caracteres especiales. No se utilizarán contraseñas que sean predecibles o deducibles con facilidad; así mismo, al ingresar las contraseñas, no se utilizarán las opciones de guardado y recordatorio automático de las mismas.

c) Los servidores deberán ejecutar siempre el cambio de contraseña la primera vez que ingresen a un servicio informático; así como según corresponda conforme establezcan los procedimientos al respecto.

d) Los servidores deberán mantener la confidencialidad y uso responsable de las contraseñas que utilizan para el acceso a información empresarial; por lo tanto, no deberán ser compartidas, ni dejarlas expuestas en lugares visibles o de fácil acceso. En todo caso, la responsabilidad por las acciones realizadas serán exclusivas de quienes sean custodios y se les haya asignado las mismas.

7.- Control de Acceso al Código Fuente

a) Solo los servidores de la Gerencia de Tecnología de Información de la Empresa, que para el desempeño de sus funciones y que hayan sido autorizados tendrán acceso al código fuente de acuerdo a sus funciones. En caso de terceros con una relación contractual o convenio con la Empresa será necesaria la autorización respectiva y del Dueño de Datos.

b) Los archivos con código fuente no deben residir en los ambientes de producción, en casos excepcionales que requieren mantenerse en producción el código fuente no debe ser visible al usuario final y de ser posible deberán ser administrados mediante una librería de programas fuentes.

8.- Seguridad física y ambiental

a) Las áreas que manejan información estratégica y sensible deberán contar con controles de ingreso físico que aseguren el acceso únicamente de personas autorizadas; siendo responsabilidad de los servidores de la Empresa hacer uso responsable de los mismos; y, las áreas competentes deberán gestionar los sistemas y permisos relacionados acorde a los procedimientos que se establezcan al respecto.

b) Áreas críticas como centros de cómputo, centros SCADA, laboratorios que disponen de equipos especializados; entre otras, y que procesen información Altamente Restringida, deberán contar con controles de condiciones ambientales, de detención y control de incendios, según corresponda para la protección de la información física y electrónica. Terceros autorizados ingresarán a éstas áreas cuando sea estrictamente necesario, siempre acompañados de un servidor autorizado de la Empresa y deberán registrar sus datos, motivo de acceso, persona que lo acompaña, fecha y hora de ingreso y salida.

9- Seguridad de los equipos

a) Los servidores son responsables del cuidado y custodia de equipos informáticos y dispositivos móviles empresariales que se les ha asignado para el desempeño de funciones, deberán ser proactivos en sus actos con la misma diligencia que emplean en la custodia de sus propios recursos para evitar los riesgos de hurto, robo o destrucción; velar por su conservación así como de la información en ellos contenida y no exponerlos a condiciones de inseguridad física, ni dejarlos desatendidos en sitios públicos cuando requieren ser movidos fuera de las instalaciones de la Empresa.

b) Los computadores de escritorio empresariales no serán reasignados a otros servidores, reubicados físicamente al interior de las instalaciones de la Empresa o fuera de la misma, a menos que se haya reportado

y coordinado las acciones pertinentes con el área de soporte de la Gerencia de Tecnología de Información y la Unidad Bienes Muebles e Inmuebles.

c) Los equipos portátiles o dispositivos móviles empresariales, por su naturaleza podrán ser movilizados dentro de las instalaciones de la Empresa para el cumplimiento de funciones asignadas bajo responsabilidad del custodio, y; por otro lado, estos equipos podrán ser trasladados fuera de las instalaciones de la Empresa siempre que los custodios a cargo de los mismos cuenten con la autorización de su jefatura inmediata con la justificación respectiva relacionada al desempeño de sus funciones.

d) En caso de robo, pérdida o daño de equipos informáticos y dispositivos móviles empresariales, los servidores responsables de su custodia lo reportarán a las áreas competentes y cumplirán con las acciones pertinentes.

e) Los equipos informáticos que soportan los procesos empresariales deberán contar con mantenimientos preventivos periódicos, protección frente fallas de energía eléctrica, únicamente con software autorizado a nivel empresarial, sistema operativo actualizado; así como antivirus y otros que la Empresa implemente para la protección de los mismos y de la información en ellos contenida.

f) Los servidores que usen dispositivos móviles empresariales serán responsables por la instalación y uso de aplicaciones que no han sido autorizadas por la Empresa y deberán reportar a soporte de la Gerencia de Tecnología de Información cualquier novedad o requerimiento al respecto.

g) Previo el proceso de baja, devolución a proveedores o reasignación de equipos informáticos o dispositivos móviles, se deberá realizar el respaldo, transferencia o eliminación segura de información empresarial y del software instalado, según corresponda.

10.- Escritorios y pantallas limpias

a) Todos los servidores no deberán dejar desatendidos sobre sus estaciones de trabajo o en lugares de fácil acceso documentos o dispositivos móviles de almacenamiento que contengan información clasificada con nivel Restringida o Altamente Restringida; en el caso de terceros autorizados, el administrador de contrato o convenio, tutor, director o coordinador deberán transmitirles este lineamiento también para su cumplimiento.

b) Cuando se imprima un documento que contenga información clasificada como Restringida o Altamente Restringida, la persona autorizada para ver esta información deberá atender todo el proceso de impresión desde el inicio y retirarla inmediatamente se concluya la impresión.

c) Al ausentarse de su estación de trabajo los servidores deberán bloquear sus computadores y protegerlos con claves de acceso; así mismo, se deberá activar automáticamente el protector de pantalla con clave si el equipo no presenta actividad en el tiempo que se establezca en los procedimientos de configuraciones y administración del Directorio Activo de la Empresa.

11.- Seguridad de la información en la relación con los proveedores y otros terceros

a) Previo a la asignación de acceso a información empresarial estratégica y sensible y por tanto confidencial a un proveedor autorizado (siempre que se justifique para cumplimiento contractual) y otros terceros, se tomarán las medidas pertinentes para su protección y asignación del perfil con los permisos estrictamente necesarios acorde a las Políticas Internas Específicas 4 y 7 de este documento. Así como, se suscribirán Acuerdos de Confidencialidad y Buen Uso de la Información; excepto cuando el requerimiento sea de Alcaldía, Secretaría de Ambiente, Secretaría de Territorio, Hábitat y Vivienda, Secretaría de Planificación y en los casos en que la ley o la Gerencia General determinen lo contrario, en estos casos hará la entrega de información el Dueño de Datos informando acerca de la Clasificación de la información y las consideraciones de seguridad.

b) En los Acuerdos de Confidencialidad, quedarán especificadas las responsabilidades para cada una de las partes, la información motivo de entrega, las consideraciones de autorización para su manejo, el tiempo de vigencia, entre otros aspectos.

c) El manejo de la información entregada se llevará según lo establezca el Acuerdo de Confidencialidad y Buen uso de información, dejando evidencia de las actuaciones que se ejecuten y considerando las condiciones del contrato, convenio, etc.

12.- Política Interna Específica: - Privacidad y protección de datos personales

En concordancia con la legislación vigente ecuatoriana y demás reglamentación que sea de obligatorio cumplimiento para la Empresa, con la finalidad de garantizar los derechos y libertades de las personas, la información que se gestione tanto en ambientes productivos como de pruebas y/o calidad concerniente a datos personales de servidores, clientes y terceros que no deba ser publicada por requerimiento de ley, será protegida para evitar su divulgación, uso o modificación no autorizados o inadecuados; igual consideración se aplicará para el manejo de información durante auditorías.

13.- Propiedad Intelectual

La utilización de software y productos de marca registrada deberán contar con su respectiva licencia para su uso en ámbitos laborales en ambientes productivos en equipos informáticos y dispositivos móviles de la Empresa. Así mismo, deberá existir un inventario actualizado del software y licencias que la Empresa ha adquirido, a cargo de Tecnología de la Información.

a) La utilización de software y productos no autorizados o no licenciados por la Empresa en equipos informáticos y dispositivos móviles de terceros autorizados que accedan a la red empresarial o red para invitados, será de exclusiva responsabilidad del tercero.

b) En los contratos que se celebren con terceros para el desarrollo de software personalizado a la Empresa en los cuales se incluye el código fuente del aplicativo, éste desarrollo es decir el código fuente se considerará como propiedad intelectual de la Empresa y se deberán especificar entre otros los siguientes puntos: Alcance de las licencias, derechos de propiedad del código desarrollado y derechos de propiedad intelectual, requerimientos de calidad, integridad y seguridad del código.

c) El software, aplicaciones y personalizaciones que se desarrollen por los servidores autorizados de la Empresa, son de propiedad de la misma.

d) La transferencia a terceros de software desarrollado en la Empresa se lo deberá realizar a través de convenios interinstitucionales.

14.- Prevención de fuga de información

a) De acuerdo al nivel de clasificación de información, para aquella que corresponda a niveles Restringida o Altamente Restringida, en los computadores de usuarios finales que la gestionen, se implementará la protección de esta información en lo que respecta a su movimiento, conforme la capacidad disponible de este sistema, para lo cual los Dueños de Datos definirán los permisos que otorgarán a los servidores que manejan esta información.

b) Los movimientos inusuales y de un número excesivo de archivos de información (mayor a 100 archivos), se reportarán dentro del horario laboral a los Dueños de Datos para su análisis y acciones pertinentes por parte del Departamento Seguridad de la Información.

15.- Gestión de incidentes de Seguridad de la Información

En el sistema de Seguridad de la información, se deberán establecer los procedimientos y demás documentación para la gestión de incidentes de Seguridad de la Información en sus etapas, para lo cual las áreas involucradas participarán conforme sus ámbitos de competencia y de acuerdo a los roles y responsabilidades que establezcan al respecto.

16.- Seguridad de la Información en la Continuidad del negocio

Con el objetivo de que se mantengan la Seguridad de la Información en ambientes de contingencia, los requisitos de Seguridad de la Información deberán considerarse en las diferentes etapas de la Gestión de continuidad de la Empresa y otros planes relacionados, es decir en la planificación, implementación, verificación y evaluaciones periódicas.

II.- Políticas Internas Específicas de Seguridad de la Información: De Aplicación para la Gerencia de Tecnología de Información

1.- Gestión de cambios en la infraestructura, servicios y sistemas informáticos

Los cambios que afecten a la Infraestructura de Tecnología y Servicios Informáticos en producción, deberán ser autorizados y gestionados siguiendo los lineamientos y procedimientos que se establezcan al

respecto para asegurar que no se afecte la confidencialidad, integridad y disponibilidad de la información para lo cual, la Gerencia de Tecnología de Información:

a) Receptará las solicitudes de cambios a los servicios y sistemas informáticos requeridos por las distintas Gerencias, realizará el análisis a las que sean consideradas viables y en base a la dificultad del cambio, definirá si la ejecución amerita la intervención de un tercero (proveedor).

b) Definirá la prioridad de atención a la solicitud de cambio de acuerdo a la urgencia e impacto de la misma en las actividades de la EPMAPS, así como también a los recursos que el cambio requiera para su implementación (interna o con terceros).

c) Deberá observar el cumplimiento obligatorio por parte del ejecutor del cambio (interno o terceros), de políticas y procedimientos de Seguridad de la Información que se relacionen con el acceso, modificación, cambio, entrega y otros aspectos respecto al manejo de información empresarial.

d) Los cambios que no generen mayor impacto en la Empresa o sean repetitivos y ejecutados por servidores autorizados de los Departamentos de la Gerencia de Tecnología de Información, se catalogarán como cambios tipo estándar, mismos que se definirán, autorizarán por los Dueños de Datos y se podrán establecer procedimientos para su ejecución cumpliendo lineamientos de Seguridad de la Información.

e) Para los cambios que impliquen la afectación a uno o más procesos de una o varias áreas de la Empresa y que no correspondan a cambios estándar previamente establecidos y aprobados, se conformará una Comisión de gestión de cambios conformada por: Gerente de Tecnología, responsables de los procesos involucrados, Dueño de Datos, jefatura del área requirente, delegado técnico, Oficial de Seguridad de la Información o su delegado; la cual analizará y aprobará o negará la solicitud.

f) Los ejecutores del cambio (internos o terceros), deberán entregar toda la documentación sobre por el cambio que han realizado en los servicios y sistemas de la Empresa, así como también deberán cumplir con la capacitación a los usuarios finales en los casos que se requiera y aplique.

g) Todos los cambios que se encuentren en ejecución ya sea por parte de terceros o por servidores de la Gerencia de Tecnología de Información, se deberán realizar en un ambiente controlado como Desarrollo y/o Calidad para su paso posterior a producción y contarán con la autorización del Dueño de Datos de tal manera que no se afecte la disponibilidad de los ambientes productivos. De forma excepcional, este lineamiento podría no ser aplicado, siempre y cuando se cuente con el informe justificativo de Tecnología de Información aprobado por el Dueños de Datos y cumplimiento lineamientos de Seguridad de la Información.

h) Para que un cambio se considere como finalizado, se deberá contar necesariamente con la aprobación de pruebas de las áreas usuarias y Dueños de Datos, así como los demás documentos que se establezcan en los procedimientos de cambios y/o pasos a producción.

i) Cuando un cambio previamente aprobado haya sido puesto en producción y por cualquier motivo genere inconvenientes en las actividades de la Empresa, operación de los sistemas u otros problemas, Tecnología de Información deberá retornar de manera inmediata a la versión anterior al cambio y reportarlo inmediatamente al Dueño de Datos.

2.- Protección contra código malicioso

a) Los equipos informáticos y dispositivos móviles con acceso a las redes empresariales IT y OT, deberán tener instalado, habilitado, activo y actualizado el software compatible para identificar, alertar sobre la presencia de código malicioso y eliminarlo.

b) Periódicamente se deberán revisar los equipos informáticos empresariales que soportan los procesos de la Empresa, a fin de determinar la presencia de archivos o software no autorizado.

c) Los servidores de la Empresa no deberán instalar en los equipos informáticos empresariales cualquier tipo de software a menos que hayan seguido el procedimiento para autorización e instalación del mismo.

d) Todo software y archivos descargados de fuentes ajenas a la Empresa, a través de Internet o cualquier otra red pública o medio electrónico, deberán ser explorados y analizados con el software contra código malicioso,

antes de que el software y los archivos sean utilizados.

e) Se deberán gestionar las vulnerabilidades técnicas de los equipos de las redes empresariales IT y OT que pueden ser explotadas por un código malicioso, como por ejemplo la aplicación periódica o cuando ameriten parches de sistema operativo y de seguridades.

3.- Respaldos de información

a) Se deberá ejecutar la operación de respaldos de la información empresarial y pruebas de recuperación e integridad por parte de los servidores responsables de esta gestión, siguiendo los procedimientos vigentes que se establezcan de acuerdo a la plataforma tecnológica respectiva.

b) Se deberán obtener al menos los siguientes respaldos y los que se especifiquen en los procedimientos respectivos:

i. Totales de información de servidores en ambientes productivos y bases de datos, anualmente al cierre del año fiscal.
ii. De los códigos fuente, de acuerdo a los cronogramas establecidos y bajo demanda cada vez que se ejecuten cambios en los mismos.
iii. Al menos semestralmente y/o cuando se ejecuten cambios de: Máquinas virtuales y discos del sistema operativo de servidores físicos que forman parte del sistema de almacenamiento empresarial.
iv. Al menos anualmente y/o cuando se ejecuten cambios de configuraciones de equipos de networking y comunicaciones.

c) El tiempo de retención de los respaldos de información empresarial será definido por los Dueños de Datos.

d) Los respaldos de información empresarial en medios de almacenamiento se deberán mantener fuera de las instalaciones del data center de la Empresa en un sitio físicamente establecido con las medidas de seguridad y condiciones adecuadas; su transporte deberá ser realizado en forma segura siguiendo los procedimientos que se establezcan al respecto.

e) La información y el software respaldados en medios de almacenamiento por más de 10 años, deberán probarse por muestreo por lo menos una vez cada dos años.

4.- Sincronización de registros

Los relojes de todos los equipos informáticos empresariales deberán sincronizarse con una sola fuente de tiempo de referencia.

5.- Ambientes de desarrollo, pruebas y producción

a) Para el procesamiento de información se contará con ambientes de desarrollo, prueba (calidad) y producción y se seguirán los procedimientos que se establezcan al respecto para el paso controlado de uno a otro.

b) En el ambiente de producción no se realizarán directamente pruebas, instalaciones o desarrollos, a menos que excepcionalmente se justifique la imposibilidad de realizarlo en los otros ambientes y se cuente con la autorización de Gerente de Tecnología de Información y en conocimiento del Dueño de Datos.

c) Los datos que se utilicen para pruebas deberán ser elegidos cuidadosamente, protegidos, controlados y manejados cumpliendo la normativa legal que aplique; se evitará el uso de datos reales y en los casos que se haga uso de éstos existirá la autorización de Tecnología de Información, Dueño de Datos y de aplicar el ente competente de protección de datos personales.

6.- Desarrollo de Software

a) Tecnología de Información podrá desarrollar nuevo software o realizará cambios al software existente que la Empresa requiera, siguiendo los procedimientos establecidos, de acuerdo al Portafolio de servicios informáticos que constan en el PETI y al Plan Anual conforme la disponibilidad de los recursos necesarios.

b) Tecnología de Información podrá adquirir software, siempre que cuente con los recursos necesarios y podrá ser para: Desarrollo de software a medida o software propietario que requiera personalización conforme las necesidades de la Empresa.

c) Las áreas requirentes presentarán justificadamente la necesidad de contar con un software que apoye su gestión, misma que deberá ser evaluada por Tecnología de Información, que a su vez informará sobre la

factibilidad de atención, propondrá la o las posibles soluciones y en coordinación con el área requirente, las demás áreas y Dueños de Datos de la información involucrada, seleccionarán la alternativa más adecuada para dar atención al requerimiento.

d) Tanto los desarrollos internos como los que se realicen a través de un tercero, deberán seguir un estándar de desarrollo que permita generar productos de software seguros y de calidad, salvaguardando la confidencialidad, integridad y disponibilidad de la información empresarial; y considerarán dentro de sus requisitos, los de Seguridad de la Información desde las etapas de diseño y posteriores hasta pruebas y puesta en producción.

e) En los proyectos relacionados con desarrollo de software, se deberá aplicar el "Marco de Referencia para la Gestión de Proyectos" que la Gerencia de Tecnología de Información establezca y además se considerarán lineamientos y requerimientos de Seguridad de la Información en las diferentes etapas inclusive, en el diseño y pruebas.

f) Si la solución que Tecnología de Información plantee incluye el desarrollo y uso de aplicaciones para dispositivos móviles, durante el análisis con el requirente, Dueños de Datos y áreas involucradas explicará detalladamente los requerimientos de recursos necesarios para la aceptación respectiva; y así mismo garantizará la seguridad de estos aplicativos.

g) El desarrollo de software deberán realizarse en ambientes de desarrollo y posteriormente se realizará su paso al ambiente de producción siguiendo los procedimientos relacionados que se establezcan al respecto, siempre que se hayan cumplido y documentado previamente las pruebas necesarias en cuanto a funcionalidad, seguridad, revisión de código y calidad.

h) Tecnología de Información deberá gestionar y mantener toda la documentación sobre: Desarrollo y control de versiones; así como de pruebas de recepción y aceptación de todos los desarrollos de software internos y a través de terceros.

7.- Gestión de Portales Web

La Gerencia de Tecnología de Información:

a) Deberá proveer el alojamiento respectivo para los portales web empresariales. Así mismo, ambos portales deberán contar con los servicios de protección de riesgos y ataques informáticos de tipo: DDOS, XSS, CSFR, entre otros.

b) Deberá gestionar la asignación de los perfiles de acceso predeterminados en el Software de Gestión de Contenidos (CMS) a los servidores de la Empresa que hayan sido autorizados para lectura y/o modificación de la información de los portales web empresariales.

c) Deberá validar la actualización e instalación de las últimas versiones, tanto del sistema operativo como de los complementos necesarios del servicio de alojamiento web empresarial; así como del Software de Gestión de Contenidos, los plugins que se están usando, de la configuración e indexación de los contenidos y la obtención y entrega de respaldos de la página web empresarial que se disponga bajo contrato(s) de servicio.

d) En los casos en que administre directamente el hardware y software de portales web de la Empresa, será responsable de las actualizaciones, mantenimiento y respaldos respectivos siguiendo los procedimientos que se establezcan al respecto.

La Dirección de Comunicación Social y Transparencia:

e) En conjunto con el Departamento Desarrollo de Aplicaciones deberán realizar el análisis respectivo para definir la plataforma de software de Gestión de Contenidos (CMS), en la que se implementen los portales web de la Empresa. Dicho análisis deberá responder a las necesidades y características de: Funcionalidad, seguridad, escalabilidad y administración, entre otros aspectos.

f) Será responsable de la Administración de Contenidos en los portales web de la EPMAPS y por tanto de la publicación de la información a petición de las Gerencias y Direcciones de la Empresa, siempre y cuando cumplan con los principios de imagen corporativa guardando relación con los propósitos, objetivos, misión y visión Empresariales. Queda prohibida la publicación de información que promueva la violencia, intolerancia, racismo, vicios o cualquier acto ilícito, proselitismo de ideas políticas o gremiales.

Municipio de Quito

8.- Gestión de información geográfica

a) Los perfiles de accesos a los sistemas de información geográfica (SigAPSA, BIMAPSA, SCADAAPSA) y su gestión seguirán lo establecido en la Política Interna Específica Control de acceso lógico y los procedimientos específicos al respecto, los perfiles corresponderán a propietario, editor-lector y solo lector.

b) Previo el acceso a editores terceros autorizados a las réplicas de bases que se generen para el efecto, deberá verificarse la firma del Acuerdo de Confidencialidad y Buen Uso de la información y se deberá poner en su conocimiento los lineamientos para la protección de la información a la que tendrán acceso.

c) Todas las bases de datos de sistemas de información geográfica cumplirán documentadamente con las fases de diseño, implementación, producción y mantenimiento, se cuidará que sean precisas (cartográfica y topológicamente), completas, conectadas e interoperables, empleando las herramientas tecnológicas acordes. Deberán disponer de metadatos hasta el nivel mínimo acordado, alineadas al estándar ISO19139, cumpliendo los lineamientos de Seguridad de la Información que apliquen.

d) Según la Ordenanza Municipal 0225 del 31-08-2007, las coordenadas planas del DMQ parten de la proyección TMQ (Transversa Mercator para Quito) y el Datum WGS84. Complementariamente, la coordenada vertical, mientras se establezca la ordenanza correspondiente, será la altura ortométrica sobre el Datum WGS84 con la aplicación de correcciones por ondulaciones geoidales existentes.

e) Las bases de datos de información geográfica inter-operarán con los otros sistemas; tendrán una arquitectura escalable en hardware y software. Tendrán ambientes de desarrollo, pruebas y producción (edición/mantenimiento y publicación) localmente o en la nube privada, que acrediten disponibilidad, accesibilidad y seguridad de los datos.

f) Las bases de datos de información geográfica, previa a su generación y diseño, deberán ser el resultado de una ingeniería/reingeniería de un proceso objetivo.

g) Debido al nivel de madurez de implementación y uso de las plataformas de software de sistemas de información geográfica, las mismas serán: Para el SigAPSA: ESRI, para el BIMAPSA: Autodesk y para el SCADAPSA: AVEVA.

h) La infraestructura para el funcionamiento de las bases de datos de los sistemas de información geográfica (nube, servidores, estaciones de trabajo, redes y comunicaciones) tendrá actualizaciones periódicas según la necesidad, avance y desarrollo tecnológico; posibilitará la integración, interoperabilidad, acceso y disponibilidad de los sistemas existentes, así como acreditarán la seguridad de la información.

Dado en San Francisco de Quito, Distrito Metropolitano, el 11 de Mayo de 2023.

Firmado electrónicamente por:
HUGO OTHON ZEVALLOS MORENO

Ing. Othón Zevallos Moreno
GERENTE GENERAL
EMPRESA PÚBLICA METROPOLITANA DE AGUA POTABLE Y SANEAMIENTO

Firmado electrónicamente por:
TANNYA MIREYA BALLADARES ONA
Razón:
Localización:
Fecha: 2023-05-11T09:46:05.342622-05:00

Firmado electrónicamente por:
TERESA VERONICA SANCHEZ HIDALGO

ANEXO: GLOSARIO DE TERMINOS DE POLÍTICAS INTERNAS DE SEGURIDAD DE LA INFORMACIÓN

Activo de información: Puede ser un dato o todo lo que permite: Almacenar, transportar o procesar datos que intervienen en el flujo de un proceso y que se encuentre en cualquier formato sea físico, digital o en el conocimiento de las personas, y que como cualquier otro activo de acuerdo a su valor para la Empresa necesita ser protegido.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

BIMAPSA: Building Information Modeling para Agua Potable y Saneamiento (Modelamiento de construcciones para agua potable y saneamiento).

Código Fuente: Es un conjunto de sentencias desarrolladas en un lenguaje de programación específico, que puede ser entendido por un usuario desarrollador y se traduce a un lenguaje de máquina para ser ejecutado por un computador.

Código Malicioso: Es un conjunto de sentencias de programación que tienen un fin malicioso y que provocan daños al computador, a un sistema informático, pueden extenderse en otras computadoras o en la red o en Internet, robar información, encriptar información y claves, eliminar información entre otros.

Confidencialidad: Propiedad de que la información no se pone a disposición o no se revela a individuos, entidades o procesos no autorizados.

Control de accesos: Mecanismo mediante el cual se restringe los accesos a un sistema informático, garantizando que los servidores cuenten únicamente con los accesos que requieren para el cumplimiento de sus funciones.

Derechos de Propiedad Intelectual: La Propiedad Intelectual comprende: Los Derechos de autor y derechos conexos; y, la Propiedad Industrial, (Art. 1 Ley de Propiedad Intelectual).

Disponibilidad: Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Dueño de Datos: Es el servidor que desempeñe el cargo de jefatura de Unidad, Departamento, Gerencia o Dirección que se ha identificado y según consten en el “Listado de Dueños de Datos” que se emita en el Sistema de Seguridad de la Información de la Empresa, que será responsable de determinar la clasificación de la información de acuerdo a los lineamientos de las Políticas Internas de Seguridad de la Información y velar por el mantenimiento de la confidencialidad, integridad y disponibilidad de la información.

Dispositivo móvil: Constituyen los equipos: Tablets, smartphones, iphones, etc. de propiedad de la Empresa, de servidores o terceros autorizados.

Equipo informático: Constituyen los equipos: Servidores, computadores de escritorio y laptops de propiedad de la Empresa, de servidores o terceros autorizados.

Identificador de usuario: Es el nombre con el cual se reconoce a la persona que dispone de accesos en un sistema informático; generalmente estos identificadores siguen una determinada nomenclatura.

Identificador de usuario genérico: Es un identificador de usuario que es compartido por varias personas que conocen su contraseña.

Información altamente restringida: Información que es utilizada solo por un grupo restringido de servidores para desempeñar sus funciones y que no puede ser conocida o entregada a otros servidores o terceros sin autorización especial de la Empresa a través de la Gerencia de Área o Dirección, el Comité que aplique o Gerencia General, según corresponda. En caso de ser conocida, utilizada o

modificada por personas si la debida autorización, su impacto sería catastrófico a los sistemas y/o procesos de la Empresa.

Información Estratégica y Sensible y por tanto Confidencial: Acorde a los niveles de clasificación de información para la Empresa, corresponde aquella que no es pública (y a su vez se subdivide en Información de uso interno, restringida y altamente restringida) y a la que tienen acceso sólo quienes por su necesidad de conocer para el desempeño de sus funciones están autorizados por el Dueño de Datos.

Información restringida: Es la información que es utilizada solo por un grupo específico de servidores para desempeñar sus funciones y que no puede ser conocida o entregada a otros servidores o terceros sin autorización del Dueño de Datos. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, su impacto sería grave o muy grave a los sistemas y/o procesos de la Empresa.

Información de uso interno: Es toda **i**nformación que es utilizada por el personal de la Empresa para desempeñar sus funciones en los procesos institucionales; y que no puede ser conocida por terceros sin la autorización del Dueño de Datos. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, su impacto sería menor a los sistemas y/o procesos de la Empresa.

Infraestructura tecnológica: Es todo equipo informático que soporta servicios informáticos.

Inicio de sesión seguro: Acceso a un sistema o aplicación mediante el uso de usuario y clave segura.

Integridad: Característica que salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Licencia de uso: Es un contrato entre el propietario (licenciante) del producto o software y el usuario (licenciatario) para su uso cumpliendo los términos y condiciones establecidos dentro de las cláusulas estableciendo entre otros: los derechos del licenciatario sobre una o varias copias, el plazo de cesión de los derechos, la no cesión a terceros o la no reinstalación en equipos distintos al que se instaló originalmente si aplica.

Medio removible de información: Son aquellos soportes de almacenamiento que son independientes del computador y que pueden ser extraídos de la computadora sin tener que apagarla, existe una variedad de tipos como: Disco externo, Flash memory, CD, DVD, etc.).

Nube privada: Es un tipo de modelo de implementación para el cómputo en la nube donde los recursos de TI (aplicaciones, cómputo, almacenamiento y redes), la cual permite una gran variedad de acceso en cuestión de minutos según demanda, y con pago por el uso.

Oficial de Seguridad de la Información: Conforme el Art. 2.- de la Resolución N.- 030 de 21 de marzo de 2019, corresponde al servidor que ostente el cargo de Jefe del Departamento Seguridad de la Información.

Privilegios de acceso: Son los permisos que se asignan a un identificador de usuario en un sistema informático, garantizando que las y los servidores cuenten únicamente con los accesos que requieren para el cumplimiento de sus funciones.

Producto o software propietario: Es cualquier producto o software cuya propiedad le corresponde a su autor o creador y sobre el cual el usuario tiene limitaciones para usarlo, copiarlo, modificarlo o redistribuirlo.

Red IT: De sus siglas Tecnologías de la Información, su función principal es la telecomunicación y la gestión del ciclo de vida de la información empresarial (administrativa) y del negocio. Elementos dentro de esta red por ejemplo son: Infraestructura de red, hardware, equipos informáticos, software cliente y servidor, bases de datos, etc.

Red OT: De sus siglas Tecnologías de la Operación, soportan los sistemas de control, supervisión y adquisición de datos (SCADA) de procesos industriales. Entre los componentes, se pueden mencionar:

Infraestructura de red, equipos informáticos, sensores, controladores, actuadores, software cliente, software servidor, bases de datos, etc., que gestionan datos industriales de operación.

Responsable de un proceso: Es la persona responsable del proceso que tiene autoridad y responsabilidad para el cumplimiento y mejoramiento del mismo; según se establece en el Manual de Procesos de la Empresa.

SCADAPSA: Supervisory Control And Data Acquisition para Agua Potable y Saneamiento (Control supervisor y adquisición de datos para agua potable y saneamiento).

Segmento de red: Es una parte de una red que agrupa a un determinado conjunto de equipos con servicios específicos.

Servicio informático: Incluye sistemas informáticos, aplicativos empresariales, acceso a la red, a recursos compartidos, a bases de datos, a servicios como correo electrónico, internet, etc.

SGSI: Sistema de Gestión de Seguridad de la Información.

SigAPSA: Sistema de Información Geográfica de Agua Potable y Saneamiento

Sistema de Información: Conjunto de elementos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Terceros: Es toda persona natural o jurídica, pública o privada ajena a las actividades que desarrolla la Empresa. De acuerdo a lo previsto en el presente instrumento, esta definición alcanzará a aquellas personas que reciban los servicios prestados por la Empresa, que le provean servicios, productos, colaboren con sus actividades complementarias, realicen proyectos de tesis, o en general, a todas aquellas que no participen en las actividades que desarrolla la EPMAPS y que al amparo de la Ley Orgánica de Transparencia y Acceso a la Información Pública soliciten información. En caso de que la información requerida, sea considerada como estratégica y sensible a los intereses institucionales y por tanto confidenciales, se procederá conforme a lo establecido en el literal c) de los lineamientos de la Política Interna General de Seguridad de la Información.

Teletrabajo: Es la prestación de servicios de carácter no presencial, a través de la cual la o el servidor realiza sus actividades fuera de las instalaciones de la Empresa, haciendo uso de las tecnologías de información y comunicación (TIC), tanto para su gestión como para su administración y control.

Teletrabajor: El servidor de la Empresa que habiendo sido autorizado, efectúe sus labores mediante teletrabajo con enlace virtual fuera de las instalaciones de la institución.

Usuario Administrador: Es la persona autorizada para cumplir con las tareas de administración de un servicio informático empresarial que incluyen: sistemas informáticos, infraestructura, equipos informáticos, bases de datos, etc.; para lo cual dispone de accesos con perfil de administrador.

Usuario Desarrollador: Es la persona autorizada para diseñar y desarrollar una aplicación para ordenadores, es decir, debe transcribir una necesidad en una solución informática escrita en lenguaje informático.

Usuario Final: Es la persona autorizada para hacer uso de servicios informáticos empresariales, enfocado a la ejecución de funcionalidades específicas de un proceso dentro de un sistema informático y que no dispone de accesos con perfil de administrador o desarrollador.

Municipio de Quito

POLITICA INTERNA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA PÚBLICA METROPOLITANA DE AGUA POTABLE Y SANEAMIENTO

MSGSI-PG-A05.1-01 rev01

La EPMAPS considera a la información como uno de sus activos más importantes para la creación de valor a la institución, a sus partes interesadas y el cumplimiento de objetivos estratégicos, misión y visión; por lo que, debe protegerse frente a amenazas internas, externas, accidentales o deliberadas; y, contar con mecanismos que aseguren razonablemente su confidencialidad, integridad y disponibilidad, mediante la mejora continua del Sistema de Seguridad de la Información alineado con el estándar ISO27001:2022, cumpliendo a demás con la legislación vigente aplicable a la Empresa.

Por lo indicado, existe el compromiso de asignación de los recursos necesarios basándose en los principios de soporte, defensa y promoción de una cultura de Seguridad de la Información.

En este contexto, la presente Política se cumplirá a través de los lineamientos que constan en documento adjunto y que deben ser observados y cumplidos obligatoriamente por todos los servidores de la Empresa.

Dado en San Francisco de Quito, Distrito Metropolitano, el 11 de Mayo de 2023.

Firmado electrónicamente por:
HUGO OTHON ZEVALLOS MORENO

Ing. Othón Zevallos Moreno
GERENTE GENERAL
EMPRESA PÚBLICA METROPOLITANA DE AGUA POTABLE Y SANEAMIENTO

Firmado electrónicamente por:
TANNYA MIREYA BALLADARES ONA
Razón:
Localización:
Fecha: 2023-05-11T09:44:17.228016-05:00

Firmado electrónicamente por:
TERESA VERONICA SANCHEZ HIDALGO

Municipio de Quito

LINEAMIENTOS DE LA POLÍTICA INTERNA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA PÚBLICA METROPOLITANA DE AGUA POTABLE Y SANEAMIENTO

Los lineamientos de la Política Interna General de Seguridad de la Información que deberán ser cumplidos obligatoriamente por todos los servidores de la Empresa, se describen a continuación:

a) Cumplir con las Políticas Internas General y Específicas de Seguridad de la Información, los Procedimientos y demás disposiciones que se establezcan en este ámbito, inclusive en modalidad de Teletrabajo y en las relaciones que se mantengan con terceros vinculados a la Empresa.

b) Usar la información empresarial física, digital o electrónica que sea conocida, creada, procesada o transmitida, de forma responsable para el desempeño de funciones y expresamente autorizada por los Dueños de Datos, protegiendo su confidencialidad, integridad y disponibilidad.

c) Utilizar los accesos asignados a los servicios informáticos de manera personal e intransferible, únicamente con fines autorizados y legales para el desarrollo de funciones; estando prohibido dañar, alterar o irrumpir las operaciones de los sistemas u obtener contraseñas, claves de cifrado u otro mecanismo que permitan un acceso no autorizado. La Empresa podrá revocar los privilegios de accesos en cualquier momento y en los casos que se determine la afectación a la Seguridad de la Información empresarial.

d) Verificar la suscripción de un Acuerdo de Confidencialidad previo a la entrega de información estratégica y sensible; y, por tanto confidencial de la Empresa a terceros; excepto cuando el requerimiento sea de Alcaldía, Secretaría de Ambiente, Secretaría de Territorio, Hábitat y Vivienda, Secretaría de Planificación y en los casos en que la ley o la Gerencia General determinen lo contrario.

e) Respetar los derechos de autor al almacenar datos e instalar, configurar o utilizar software en los activos informáticos de propiedad de la Empresa; así mismo, se prohíbe la transmisión, difusión o almacenamiento de información transgrediendo disposiciones legales o regulatorias como: Material protegido por derechos de propiedad intelectual, pornográfico, obsceno, difamatorio y en general aquel que impacte negativamente en la productividad, trabajo de la institución, bienes tangibles o intangibles, o que constituya una amenaza legal o tecnológica.

f) Reportar oportunamente a la Jefatura inmediata y a la cuenta de correo informacionsegura@aguaquito.gob.ec; así como también responder: Las alertas de Seguridad de la Información, avisos, sospechas de vulnerabilidades o similares; y, cooperar con el proceso de investigación de cualquier incidente de Seguridad de la Información que pueda dar origen a procesos administrativos, disciplinarios, civiles o penales.

g) El incumplimiento de Políticas, Procedimientos o demás lineamientos de Seguridad de la Información, estará sujeto al análisis e imposición de medidas disciplinarias de acuerdo a su gravedad siguiendo lo establecido en el Reglamento Interno de Administración del Talento Humano (RIATH) y en el Reglamento Interno de Trabajo (RIT).