INTRODUCCIÓN

EMPRESAS PÚBLICAS DEL QUINDÍO S.A (E.S.P), determina la información como un activo de alta importancia, que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información, por lo que se establece las políticas de seguridad informática, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Empresa; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. La seguridad de la información es para la Empresa, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas.

1. OBJETIVOS

Describir las políticas de seguridad informática de la EMPRESAS PÚBLICAS DEL QUINDÍO S.A (E.S.P), en especial enuncia los principales lineamientos en aspectos generales, con sistemas que apoyan la gestión de la organización, servicios informáticos, equipos de cómputo, redes de datos, seguridad informática entre otros.

2. ALCANCE

Esta política está dirigida a directivos y funcionarios en general que se beneficien con la tecnología informática de la Empresas Públicas del Quindío S.A. (E.S.P.), incluyendo personal en outsorcing o de otras Organizaciones que laboren en las instalaciones de la EMPRESAS PÚBLICAS DEL QUINDÍO S.A. E.S.P. y aplican a equipos propios, en alquiler, comodato o en cualquier tipo de convenio que incluya equipos de cómputo.

3. POLÍTICAS DE SEGURIDAD INFORMATICA

La Gerencia General debe aprobar las Políticas de Seguridad informática, demostrando así su compromiso con la seguridad de la información en la Empresa EPQ SA ESP. Una vez aprobada dichas políticas, la Alta Dirección debe velar por su divulgación y cumplimiento al interior de la empresa. La Alta Dirección debe revisar periódicamente la aplicabilidad y vigencia de las siguientes Políticas específica de Seguridad informática y efectuar los ajustes necesarios sobre ellas para que sean funcional y se pueda seguir exigiendo su cumplimiento por parte de todos los funcionarios y personal suministrado por terceras partes que provean servicios a la empresa.

4. CONDICIONES GENERALES

- El ingeniero de sistemas, será el directo responsable de este documento y su cumplimiento, de tal forma que aplique a los cambios tecnológicos que ocurran en la Empresas Públicas del Quindío S.A. (E.S.P.) o normas jurídicas que afecten las políticas aquí enunciadas.
- La Empresas Públicas del Quindío S.A. (E.S.P.) hará responsable al Usuario del conocimiento de la presente Política y las consecuencias que se derivarían de su incumplimiento. Así mismo, el Usuario deberá conocer estas políticas desde su ingreso a la organización.
- La Empresas Públicas del Quindío S.A. (E.S.P.) se reserva el derecho de evaluar periódicamente el cumplimiento de estas Políticas. Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos por la Empresas Públicas del Quindío S.A. (E.S.P.) y en estricto acato de las estipulaciones legales vigentes.
- En materia de irregularidades o incumplimiento en el uso del software, el Usuario que no cumpla con esta política, será directamente responsable de las sanciones legales (que, por responsabilidad laboral, penal y/o civil se incurra) derivadas de sus propios actos.

5. DEFINICIONES

- Hardware: Conjunto de elementos materiales que componen un ordenador. Hardware también son los componentes físicos de una computadora tales como el disco duro, CD-DVD, etc... En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, cajas, periféricos de todo tipo y otros elementos físicos.

- Software: también conocido como programática o equipamiento lógico es el conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina. Se trata del conjunto de instrucciones que permite la utilización del ordenador. El software es la parte intangible de la computadora, es decir programas, aplicaciones etc.

- Dominio: dirección de una página o recurso en Internet por la que se identifica al servidor en el que se aloja, también se usa en la terminación de los correos electrónicos corporativos.

- Navegador: Uso de la herramienta Internet, búsqueda, consulta y revisión de páginas web.

6. POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1 ORGANIZACIÓN DE LA SEGURIDAD

- Empresas Públicas del Quindío EPQ SA ESP debe definir responsabilidades y deberes con respecto a la seguridad de la información, y asegurar la concientización de funcionarios y terceros con respecto a la importancia y el cumplimiento de la normatividad definida.
- Los terceros que efectúen el Tratamiento de Información propia de la Empresa o sobre la cual la Empresa sea Responsable, deben cumplir con la Política de Seguridad de la Información.

6.2 GESTIÓN DE ACTIVOS DE INFORMACIÓN

- Cualquier funcionario o contratista que intente inhabilitar, vencer o sobrepasar los controles de seguridad de la Información en forma no autorizada será sujeto de las acciones legales correspondientes.
- Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios.
- La Empresa, se reserva el derecho de restringir el acceso a cualquier Información en el momento que lo considere conveniente.
- Los controles serán diseñados para proveer un nivel de protección de la Información apropiado y consistente dentro de la Empresa, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de

la Información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

- Está prohibido mover los equipos de cómputo de los lugares donde se encuentran o realizar cambios de equipos o periféricos como teclados, ratones o monitores con otros funcionarios. Únicamente el ingeniero de sistemas podrá realizar esta labor si fuera necesaria.

6.3 SEGURIDAD EN EL RECURSO HUMANO

- Se deben implementar capacitaciones y divulgaciones en seguridad de la información y de los procedimientos de gestión de incidentes de seguridad. Los funcionarios deben conocer la normatividad relacionada con la seguridad de la información de la Empresa ya que el desconocimiento de la misma no los exonerará de los procesos disciplinarios definidos ante violaciones de las políticas de seguridad.

6.4 SEGURIDAD FÍSICA

- Mantener Áreas seguras para la gestión, almacenamiento y procesamiento de información en la Empresa. Las áreas deben contar con protecciones físicas y ambientales acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, incluyendo la definición de perímetros de seguridad, controles de acceso físicos, seguridad para protección de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales adecuadas de operación y sistemas de contención, detección y extinción de incendios.
- El ingreso de terceros a los Centros de Cómputo y Centros de Cableado, debe estar debidamente registrado mediante una bitácora custodiada por el personal de vigilancia de la Empresa.
- Los privilegios de acceso físico a los Centros de Cómputo deben ser descontinuados o modificados oportunamente a la terminación, transferencia o cambio en las labores de un funcionario autorizado.
- El Centro de Cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, sistema de alarmas o controles biométricos; sistemas de detección y extinción automáticas de incendios, control de inundación y alarmas en caso de detectarse condiciones inapropiadas, estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.
- Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

- Los funcionarios o terceros que presten sus servicios a la Empresa, no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.
- La seguridad de los equipos de cómputo fuera de las instalaciones será responsabilidad de a cada funcionario y contratista asignado, junto con una autorización del jefe inmediato.
- Los accesos a áreas seguras deberán tener un control de acceso físico, y no se debe permitir ingresar equipos fotográficos, de filmación, grabación de audio u otras formas de registro salvo con autorización especial del responsable del área segura.
- Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.
- Es responsabilidad del usuario mantener el área del equipo libre de alimentos, bebidas o cualquier otro elemento que pueda dañar la pantalla, teclado o CPU.

6.5 GESTIÓN DE COMUNICACIONES Y OPERACIONES

- Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad deben estar documentados, garantizando un adecuado control de cambios.
- A efectos de proteger la integridad y confidencialidad de los activos de información es imprescindible que se cuente con protecciones contra software malicioso, mantenimiento de los equipos, administración de la red y bloqueo de puertos en la red de telecomunicaciones.
- La Oficina de Gestión de sistemas de Información, debe garantizar los recursos necesarios que aseguren la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios que ejecutan dichas labores.
- Todos los usuarios de activos de información tecnológicos y recursos informáticos que requieran la adición o modificación de funcionalidades de los mismos, deben solicitar el cambio por medio del procedimiento vigente para dicha acción.
- Toda adquisición, mantenimiento y eliminación de medios de almacenamiento deberá ser realizada por el proceso de Gestión Sistemas de Información, de manera que se garantice seguridad en estos activos de información.

6.6 USO DEL CORREO ELECTRÓNICO

- Los servicios de mensajería electrónica son de uso exclusivo para actividades relacionadas con el negocio, por lo tanto, queda prohibido el uso del correo empresarial, para fines personales.

- Está restringido el envío de mensajes con archivos de música (mp3, wav, wvma, etc), videos (avi,mpg, mpeg, mov, etc), imágenes pornográficas (jpg, bmp, gif, tif, etc) y/o archivos con extensiones exe, com, bat, src, etc, ya que este tipo de archivos facilitan la propagación de virus e incrementan el ingreso de correos no solicitados. Igualmente está prohibido el envío de mensajes como cadenas, felicitaciones, mensajes de navidad, tarjetas o cualquier otro mensaje ajeno a las funciones y operaciones de la Empresa, que congestione la red de la empresa y que no corresponda al tema laboral.
- Se prohíbe el envío masivo de correos.
- Se prohíbe el envío de copias o reenvío de correo electrónico con información confidencial, sin el consentimiento del remitente original.
- Se prohíbe a los usuarios suscribirse a listas de correo electrónico o participar en grupos de noticias ("newgroups") que divulguen información o mensajes ajenos a las funciones y labores de la Empresas Públicas del Quindío S.A. (E.S.P.).
- Cuando escriba un correo, evite poner fondos y otros elementos "innecesarios", ya que solo hacen aumentar el tamaño del mensaje a transmitir, lo que puede ocasionar que el destinatario no lo reciba. A la hora de la firma, la cual no debería tener más de cuatro líneas, evite poner caracteres innecesarios. Es tráfico innecesario que consume recursos de la red.
- Cuando reenvíe un mensaje, coloque sus propios comentarios al principio, no al final. Esto le permite a la persona que lo recibe conocer con anterioridad el propósito de su correo
- Todo usuario del correo electrónico deberá leer y responder oportunamente los mensajes y citaciones que se le envíen por este medio; con el fin de aprovechar el mayor beneficio que ofrece el correo electrónico que es la rapidez y efectividad de las comunicaciones
- No Interferir o interrumpir el servicio, servidores, redes conectadas o el tiempo de sus compañeros de trabajo con mensajes de correo que no sean laborales, como: Mensajes en cadena, oraciones a cambio de beneficios, tótems, pornografía, chistes, videos o cualquier manifestación similar, significa entorpecer las labores diarias y esto afecta directamente el servicio con el usuario.
- Respaldar la información que se recibe por correo en forma continua y eliminar aquella que no es pertinente.
- El mail debe tener un título (subject o asunto) que refleje el contenido del mensaje.
- No abrir correos cuyo remitente le sea desconocido o cuyo asunto le resulte sospechoso.
- El usuario del Correo Electrónico tiene derecho a manejar su información en forma confidencial, asumiendo toda responsabilidad por dicho uso.
- No se permite utilización de smileys.

6.7 CONTROL DEL ACCESO

- Deben establecerse medidas de control de acceso al sistema operativo, para garantizar la autenticación de los funcionarios.
- Los empleados no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical. La longitud mínima de las contraseñas será igual o superior a ocho caracteres y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Se debe permitirse identificar de manera inequívoca cada usuario, dejar registro de las actividades que realiza.
- Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo de la Empresa, la interfaz del sistema operativo debe estar configurada de tal forma que tenga solo privilegios de invitado. Todas estas labores deben ser estrictamente realizadas por el proceso de Gestión Sistemas de Información.
- Todos los usuarios con acceso a un sistema de información o a la red informática de la Empresa dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que ha sido asignado.
- El acceso a la información de la Empresa, deberá ser otorgado sólo a Usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad.
- Todos los escritorios de los funcionarios de la Empresa deben mantenerse despejado en ausencia de este.
- El escritorio virtual de cada equipo de cómputo independiente del sistema operativo que use, debe mantenerte despejado, no debe contener archivos de ningún tipo salvo los accesos directos a aplicaciones necesarias en la labor del empleado.
- Todo el personal debe bloquear el equipo de cómputo con protector de pantalla que exija la contraseña de acceso a la sesión ante la ausencia temporal del puesto de trabajo.
- Por política de Directorio Activo se debe bloquear con protector de pantalla que exija la contraseña de acceso tras 3 minutos de inactividad del equipo.
- La asignación de privilegios a las aplicaciones informáticas presentes en la Empresa, debe ser solicitada por el Líder de Proceso y/o jefe inmediato al proceso de Gestión Sistemas de Información para su ejecución.
- Si entes externos tienen acceso a información crítica de la Empresa, se deben suscribir acuerdos para la salvaguarda de la información.

6.8 SERVICIO DE INTERNET

- El acceso a Internet, solo se permitirá para operaciones relacionadas con el negocio de la Empresas Públicas del Quindío S.A. (E.S.P.). De ahí que estén prohibidas todas aquellas páginas relacionadas con apuestas, chistes, música, video, juegos, pornografía, catálogos de ventas, horóscopos, tarjetas, etc.
- El uso de salas de Chat está prohibido.
- En la empresa no está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser previamente consultada con el ingeniero de sistemas.
- Los usuarios que estén haciendo uso indebido de los recursos informáticos serán notificados a su jefe inmediato y se les suspenderá el servicio por una semana, de reincidir en la falla se le notificará a la subgerencia y el servicio será suspendido hasta nueva orden.
- Se garantizará la disponibilidad de Internet en un 90%
- Se autoriza la navegación en páginas cuyo contenido este acorde a las necesidades del negocio.
- El uso indebido de Internet es responsabilidad del usuario y se considerará una falta al reglamento interno de trabajo y será sancionado como tal.

6.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

- Empresas Públicas del Quindío EPQ SA ESP debe asegurar que se haga el diseño e implementación de los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.
- La Empresa, debe establecer controles para cifrar la información que sea considerada sensible y evitar la posibilidad de repudio de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.
- La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como el desarrollo de soluciones.
- La información tratada por las aplicaciones aceptadas por la Empresa, debe preservar su confiabilidad desde su ingreso, transformación y entrega a las aplicaciones de la Empresa.

6.10 GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Empresas Publicas del Quindío EPQ SA ESP, debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

- Todos los usuarios de la información de la Empresa deben reportar los incidentes de seguridad que se presenten, según el procedimiento vigente en la Empresa.

- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables.

6.11 GESTIÓN DE LA CONTINUIDAD DE LOS PROCESOS

- Debe evaluarse el impacto de las interrupciones que afectan la operación de los procesos críticos de la Empresa y definir e implementar planes de continuidad y de recuperación ante desastres para propender por la continuidad de la misma. Los planes deben considerar medidas tanto técnicas como administrativas para que se puedan recuperar oportunamente las funciones de los procesos y la tecnología que las soporta.

Los planes de continuidad y de recuperación deben probarse y revisarse periódicamente y mantenerlos actualizados para su mejora continua y garantizar que sean efectivos.

- Para los procesos críticos de la Empresa, se debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad de los procesos, aún en caso de desastre en las instalaciones de los lugares de Operación.

- Cada lugar debe incluir los controles establecidos para éste tipo de áreas según su clasificación, para que no se vea disminuida los aspectos de seguridad en caso de desastre.

- Se debe seguir una estrategia de recuperación alineada con los objetivos de negocio, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.

6.12 CUMPLIMIENTO

• Empresas Publicas del Quindío EPQ SA ESP, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros, la privacidad, los delitos informáticos, el uso inadecuado de recursos de procesamiento, el uso de criptografía y la recolección de evidencia.

• Cumplimiento de la normatividad y los controles relacionados con la seguridad de la información y los que son técnicamente compatibles con los diferentes ambientes o tecnologías de la empresa.

• Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la Empresa deben contar con su respectiva licencia de uso.

• Realización de auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información.

• La Política junto con el Sistema de Gestión de Seguridad de la Información de Empresas Publicas del Quindío EPQ SA ESP, debe ser auditado anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

• La información de auditoría generada por el uso de los controles de seguridad de los Recursos de Tecnología, debe ser evaluada por el Responsable para: ¬ Detectar Violaciones a la Política. ¬ Reportar incidentes de seguridad. ¬ Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

• Los contratos de trabajo y los contratos de desarrollo realizados por proveedores y contratistas deben contar con cláusulas respecto a la propiedad intelectual que le pertenece a Empresas Públicas del Quindío EPQ SA ESP.

7. RESPONSABLE DEL DOCUMENTO

SUBGERENCIA ADMINISTRATIVA Y FINANCIERA.

JAMES PADILLA GARCIA

GERENTE GENERAL

Elaboró y proyectó: Cesar Iván López B. Profesional Universitario.
Revisó: Lina Marcela Sierra Correa. Profesional Universitario de Calidad.
Aprobó:
Isabel Cristina Ortiz Cortés - Subgerencia de Planeación Y Mejoramiento institucional
Ana María Arroyave Moreno. Subgerente Administrativa y Financiera.