ESPA
Empresa de Servicios Públicos de San José de la Marinilla E.S.P.

RESOLUCIÓN No.228
OCTUBRE 16 DE 2020

POR MEDIO DE LA CUAL SE ADOPTA LA POLITICA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN TIC, EN LA EMPRESA DE SERVICIOS PÚBLICOS DE SAN JOSE DE LA MARINILLA ESP

El Representante Legal y Gerente de la Empresa de Servicios Públicos de San José de la Marinilla E.S.P. en uso de sus atribuciones legales y,

CONSIDERANDO:

a) Que la Ley 1753 del 9 de junio de 2015, mediante la cual se expidió el Plan Nacional de Desarrollo 2014-2018 "Todos por un Nuevo País", dispuso en el parágrafo 2 literal b) del artículo 45, que: "las entidades estatales tendrán un Director de Tecnologías y Sistemas de Información responsable de ejecutar los planes, programas y proyectos de tecnologías y sistemas de información en la respectiva entidad. Para tales efectos, cada entidad pública efectuará los ajustes necesarios en sus estructuras organizacionales, de acuerdo con sus disponibilidades presupuestales, sin incrementar los gastos de personal. El Director de Tecnologías y Sistemas de Información reportará directamente al representante legal de la entidad a la que pertenezca y se acogerá a los lineamientos que en materia de TI defina el MinTIC".

b) Que la RESOLUCIÓN N° 034 De Marzo 04 de 2016 estableció en LA EMPRESA DE SERVICIOS PÚBLICOS DE SAN JOSÉ DE LA MARINILLA E.S.P., la cartilla de Políticas de Información y Comunicación.

c) Que la RESOLUCIÓN No.207 SEPTIEMBRE 16 DE 2020 "POR LA CUAL SE ADOPTA EL PLAN DE COMUNICACIONES".

d) Que el Departamento administrativo de la Función Pública considera que las entidades, independientemente de la organización o estructura con la que cuenten para el cumplimiento de las funciones relacionadas con tecnologías de la información y las comunicaciones, deben implementar estrategias para el fortalecimiento institucional en la materia

e) Que el Gobierno Nacional expidió el Decreto 415 del 07 de Marzo del 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

En merito a lo expuesto resuelve.

RESUELVE:

Artículo 1o. Adoptar LA POLITICA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN TIC, que se describe a continuación:

Política ESPA, de Tecnologías de Información y Comunicación TIC

- Política de adquisición, implementación y mantenimiento de las TIC
- Política de uso para equipos portátiles y dispositivos móviles
- Política de gestión de servicios TIC
- Política de manejo y protección de la información
- Política de responsabilidad en el uso de las TIC
- Política de soporte a los usuarios de las TIC
- Política de relación con infraestructura de terceros
- Política de gestión del riesgo TIC
- Política de incorporación al cumplimiento regulatorio
- Política de protección del medioambiente
- Política de seguridad de la información

ALCANCE

Establecer un marco de gobierno para que el uso de las TIC's de la organización, logre satisfacer las necesidades actuales y futuras derivadas de la estrategia de la institución, siguiendo los

criterios de innovación, calidad, eficiencia, escalabilidad. Estas políticas son aplicables a todos los colaboradores, consultores, contratistas, terceras partes, que usen las tecnologías de información y la comunicación de la organización.

LINEAMIENTOS GENERALES DE LA POLÍTICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

Responsabilidad: Es responsabilidad del Comité de gobierno digital, hacer uso de la política de TIC como parte de sus herramientas de gobierno y de gestión y definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

Cumplimiento: El cumplimiento de la Política de Tecnologías de la Información y Comunicación (TIC) es obligatorio. Si los colaboradores, consultores, contratistas, terceras partes violan estas políticas, la Organización se reserva el derecho a tomar las medidas correspondientes.

Excepciones: Las excepciones a cualquier cumplimiento de Política de Tecnologías de la Información y Comunicación (TIC) deben ser aprobadas por el Comité de gobierno digital. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas por dicho Comité.

Administración de las políticas: Las modificaciones o adiciones de la Política de Tecnologías de la Información y Comunicación (TIC) serán propuestas y atendidas por el Comité de gobierno digital. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

DEFINICIONES

Para los propósitos de este documento, se definen los siguientes conceptos:
Activo: Cualquier cosa que tenga valor para la Organización.
Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la Organización.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Continuidad: Capacidad de la Gestión de Servicios de Tecnología para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.

Desastre o contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma, por medio de equipos de cómputo u otros medios necesarios para la operación normal de un negocio.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de un proceso autorizado.

La Organización: Se refiere a la Espa. (Empresa se servicios públicos de San José de la Marinilla ESP)

Evaluación del Riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos.
Impacto: La consecuencia que al interior de la compañía se produce al materializarse una amenaza.

Operación: Actividades diarias de infraestructura realizadas para soportar y entregar los servicios de tecnología.

Políticas: Toda intención y directriz expresada formalmente por la administración de la Organización.

Procesos: Se define un proceso empresarial como conjunto de actividades que reciben una o más entradas para crear un resultado/producto de valor para el cliente o para la propia compañía/proceso (concepto de Cliente Interno de Calidad). Normalmente, una actividad empresarial cuenta con múltiples procesos que sirven para el desarrollo de su objeto empresarial.

Procedimientos: Pasos operacionales que los colaboradores deben realizar para alcanzar ciertos objetivos/resultados.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Puede involucrar otras propiedades como autenticidad, trazabilidad, y fiabilidad.

TIC: Se refiere a las Tecnologías de Información y Comunicación.
Vulnerabilidad: Debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

Comité de Gobierno Digital: permitan contar con entidades públicas más proactivas e innovadoras para garantizar mejores condiciones de vida a los ciudadanos, así como satisfacer necesidades

y problemáticas a través del aprovechamiento de las tecnologías de la información y las Comunicaciones. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2), Ministerio de Tecnologías de la Información y las Comunicaciones.

POLÍTICA DE ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE LAS TIC

El comité de gobierno digital, es el responsable de la adquisición, instalación y mantenimiento de todos los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), requeridas para los procesos de la Organización, buscando, dentro del marco legal que rija, asegurar la calidad de los servicios entregados y de acuerdo con criterios de innovación, confiabilidad, disponibilidad, seguridad, economía e interoperabilidad, que den soporte a la productividad de los colaboradores en los procesos.

Estándares de la Política de adquisición, implementación y mantenimiento de las TIC

Requerimientos tecnológicos: Cuando un área requiera implementar un software, plataforma tecnológica o sistemas de información, debe diligenciar el respectivo formato de requerimientos y asignar a una persona responsable para liderar la implementación solicitada.

Para el manejo y administración de los requerimientos tecnológicos (adquisiciones, implementación y mantenimiento), los dueños de los procesos de la Organización tienen la responsabilidad de verificar la funcionalidad de lo implementado.

Desarrollo de aplicaciones: Las aplicaciones que desarrollen terceros para la empresa deben cumplir con los requerimientos de seguridad establecidos por la Organización conforme con la Política de Seguridad de la Información, que se desarrolla más adelante en este documento.

La propiedad intelectual de los desarrollos contratados o realizados por los terceros dentro de su trabajo será propiedad de la Organización, salvo acuerdo escrito expreso que diga lo contrario.

Los colaboradores o terceros que tengan acceso a los sistemas TIC de la Organización, no podrán copiar ni ceder sin autorización las aplicaciones que son propiedad de la compañía ni las aplicaciones o programas de los que esta tenga licencia de uso.

Procesos de desarrollo y soporte: El proceso de adquisición y desarrollo de las aplicaciones debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones.

La documentación de cada uno de los sistemas implantados en la empresa debe contener la guía para brindar soporte, la cual incluya copia del contrato con el proveedor que lo brinda, en caso

de que aplique esta modalidad, especificando los Acuerdos de Nivel de Servicio (ANS) establecidos, los interlocutores y los procedimientos para obtener el servicio.

Seguridad en los archivos del sistema: El acceso a los archivos del sistema y al código fuente debe ser restringido. La actualización del software aplicativo y las librerías solo pueden ser llevadas a cabo por los administradores, considerando que para software de proveedores las actualizaciones y migración a nuevas versiones se deben realizar antes de que termine la vigencia del soporte.

Los procedimientos de control de cambios deben estar documentados y ser ejecutados bajo los controles adecuados para no comprometer la seguridad de los sistemas.

Controles criptográficos: La implementación de controles criptográficos se realiza con base en una evaluación de riesgos que identifique el nivel de protección necesario, teniendo en cuenta el tipo, la fortaleza y la calidad del algoritmo de cifrado requerido.

INFRAESTRUCTURA INFORMÁTICA

Responsabilidades de la operación: Los procedimientos de operación deben considerar la planeación de la operación, el tratamiento y manipulación de la información, las copias de respaldo, el manejo de errores o excepciones durante la ejecución de un trabajo, los contactos de apoyo para el caso de dificultades operacionales o técnicas inesperadas, reinicio de los sistemas y procedimientos de recuperación a utilizar en caso de falla del sistema.

Separación de ambientes: Para minimizar los riesgos en el proceso de incorporación de cambios y nuevos desarrollos, así como el impacto por la no disponibilidad de los servicios, se debe establecer una segregación de ambientes, considerando:

- El uso de diferentes equipos, dominios y directorios.
- El uso de perfiles de usuario diferentes para los diferentes ambientes.
- La restricción de uso de datos de producción en ambientes de prueba.

Planificación y aceptación: Se deben establecer proyecciones de capacidad futura, para reducir el riesgo de sobrecarga del sistema.

Se hará monitoreo al uso de los servicios de red y de los sistemas, con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con los Acuerdos de Niveles de Servicio y reducir el riesgo de posibles fallas.

Protección contra códigos maliciosos: Se deben implementar controles de detección, prevención, recuperación y concientización, con el fin de que los usuarios tengan protección frente a códigos maliciosos.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y acorde con la propiedad intelectual.

Gestión de seguridad en las redes: Las redes y la infraestructura de apoyo deben ser adecuadamente gestionadas y aseguradas para protegerlas de amenazas y para mantener la seguridad de los sistemas y aplicaciones.

Se deben implantar controles relacionados con la segmentación, gestión, monitoreo y detección de eventos, para asegurar la información que viaja por las redes.

Manejo de los medios magnéticos: Se deben establecer procedimientos adecuados para proteger los medios magnéticos, para prevenir la revelación, modificación, eliminación o destrucción no autorizada.

Debe existir un inventario de medios magnéticos y deben almacenarse de acuerdo con las prescripciones del fabricante para prevenir la pérdida o deterioro de la información.

Todos los medios deben ser etiquetados de acuerdo con el procedimiento de clasificación y manejo de la información establecido por la compañía.

Los medios se deben de proteger contra el acceso no autorizado, el mal uso o corrupción, durante el transporte fuera de los límites físicos de la empresa. Esto se hace por medio de transportes autorizados.

TELECOMUNICACIONES

Uso de las Redes: El área de Tics, es la responsable de definir las necesidades que tiene la compañía con respecto a las redes (alámbricas e inalámbricas). Es responsable también de la administración de los anchos de banda necesarios para soportar los servicios TIC, incluyendo antenas externas.

El uso de las redes será monitoreado con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con los Acuerdos de Niveles de Servicio y reducir el riesgo de posibles fallas.

Cualquier solicitud de servicio que no pueda ser soportada por la infraestructura existente debe negociarse con el área respectiva y seguir los estándares de implementación.

Telefonía fija: La asignación de extensiones telefónicas y modificación de categorías de acceso telefónico se hará de acuerdo con el perfil configurado en la matriz de atributos.

El uso de los teléfonos fijos asignados a los colaboradores debe ceñirse al desarrollo de actividades relacionadas con el cargo.

•Todos los servicios, requerimientos o incidentes, después de pasar por los niveles de autorización establecidos, serán canalizados por medio del comité de gobierno digital y/o aprendiz, hacia el proveedor de outsourcing de telecomunicaciones.

Para control y seguimiento se debe generar un reporte periódico de consumo telefónico y comunicarlo a las debidas instancias para su respectivo análisis.

Telepresencia: La compañía dispone de software de control remoto para establecer contacto virtual entre los colaboradores de las diferentes sedes, permitiendo acortar distancias y hacer más eficientes los procesos.

Algunos colaboradores disponen del aplicativo Team viewer, el cual permite realizar control remoto facilitando la colaboración y participación desde cualquier lugar.

POLITICA DE USO PARA EQUIPOS PORTÁTILES Y DISPOSITIVOS MÓVILES

El área de las Tics, establece los requisitos y controles para la conexión de equipos portátiles y los dispositivos móviles a la red de la compañía.

Los colaboradores, consultores, contratistas y terceras partes, podrán hacer uso de los dispositivos móviles, siempre y cuando cumplan con los criterios técnicos, funcionales, de seguridad, regulatorios y económicos establecidos por la Organización.

Estándares de la Política para equipos portátiles y dispositivos móviles

Asignación y uso de teléfonos celulares: La empresa cuenta con un plan corporativo de servicios de telefonía móvil suministrado por un operador determinado. Comité de gobierno digital es responsable de la contratación del servicio de telefonía celular con el prestador de servicios que

garantice las mejores condiciones para la empresa, en términos de servicios, costos, planes y cobertura.

La asignación de los equipos y planes de telefonía celular para los colaboradores se realiza de acuerdo con las responsabilidades y con la aprobación del comité respectivo. La entrega de los equipos celulares se hace únicamente con los accesorios originales propios de cada teléfono y de acuerdo con los modelos correspondientes al plan o servicio contratado.

El área de Tics, tiene bajo su responsabilidad el suministrar la ayuda en lo que se refiere a configuración de las aplicaciones y servicios autorizados por la compañía, todo otro soporte es responsabilidad exclusiva del colaborador.

El colaborador que cuente con servicio de telefonía celular, asignado por la compañía, debe respetar el valor del plan establecido y atender los criterios de racionalidad y disciplina en el uso del servicio. Igualmente, debe ser utilizado por el colaborador para realizar las funciones establecidas para su cargo y su uso debe estar orientado a agilizar las funciones inherentes al mismo.

En el caso de pérdida, hurto, o daño del equipo, con excepción del deterioro normal, su reposición, reparación o mantenimiento es responsabilidad del colaborador. Así mismo, el colaborador debe notificar la pérdida o mal estado en un término no superior a 48 horas.

El comité, siempre revisa los consumos de voz y datos de cada colaborador al que se le ha asignado la línea de la empresa y aquellos valores que sobrepasan los límites autorizados son validados con el Coordinador respectivo y deducidos por nómina si no hay una justificación al respecto.

El colaborador que se retire de la empresa, debe proceder con el trámite de realizar la entrega del equipo con su respectiva línea.

Planes de datos: Los colaboradores con plan de datos asignado, deben dar un uso racional y estrictamente laboral a este. No deben realizarse labores que generen costos adicionales ni descargar software no autorizado en los dispositivos que cuenten con plan de datos pagado por la compañía.

Así mismo, deben acogerse las disposiciones de navegación definidas por la compañía, las cuales prohíben, entre otros, la consulta de páginas violentas, pornográficas o que atenten contra los principios, ética y moral de los colaboradores.

El incumplimiento por parte de los colaboradores de lo dispuesto en esta Política, dará lugar a las sanciones previstas en el Código Sustantivo del Trabajo, el Reglamento Interno de Trabajo, el Contrato de Trabajo Individual y en otras leyes y normas que resulten aplicables.

Utilización de Internet móvil: La empresa asigna servicio de Internet móvil a los colaboradores que por motivos del servicio lo requieran y deben permanecer en lugares donde resulta difícil la comunicación.

Es responsabilidad de los colaboradores hacer un uso adecuado de éste servicio. Asimismo, deben acogerse las disposiciones de navegación definidas por la compañía que prohíben la consulta de páginas violentas, pornográficas o que atenten contra los principios, ética y moral de los colaboradores.

POLÍTICA DE GESTION DE SERVICIOS TIC

El área de Tics, promueve la adopción de un enfoque basado en procesos integrados, de modo que se entreguen servicios oportunos, efectivos, eficientes y funcionales.

Estándares de la Política de gestión de servicios TIC

Acuerdos de Niveles de Servicio (ANS): Considerando los requisitos del cliente interno, los requisitos legales y reglamentarios, el área de Tecnología de la Información y las Comunicaciones, dispone de un catálogo que recoge todos los servicios ofrecidos a sus clientes internos.

Los Acuerdos de Nivel de Servicio deben ser el resultado de las negociaciones con el cliente interno y serán soportados por los Acuerdos de Nivel de Servicio Operativo y con los proveedores.

La gestión de ANS se soporta por medio del protocolo de Niveles de Servicio.

Mejora Continua: El seguimiento a los Acuerdos de Nivel de Servicio permitirá medir la efectividad y la eficiencia de los servicios de tecnología y comunicaciones. Con los resultados obtenidos se plantean las acciones que permiten mejorar continuamente los servicios.

La mejora continua tiene como fundamento los siguientes principios (elaborar encuesta de satisfacción del cliente interno):

- Mejorar de manera continua los servicios y los procesos.
- Corregir cualquier falta de conformidad en el servicio o con los planes de gestión.

Calle 30 No 25-96
PBX (4) 548 7116 - 548 2811
www.espamarinilla.gov.co
Marinilla - Antioquia
Nit 811 014 470-1
Vigilado SSPD

- Asignar eficazmente las funciones, recursos y responsabilidades relacionados con la mejora del servicio.

La Gestión del Servicio debe canalizar, registrar, priorizar y solicitar la debida autorización de las mejoras recibidas. Una vez aprobadas las mejoras, deben quedar registradas en el Sistema de Mejoramiento de la Calidad de la Organización, para su posterior seguimiento e implantación (ACPM).

Gestión financiera: La política financiera se fundamenta en las siguientes directrices:

- Disponer de unos presupuestos que sean equilibrados y adecuados con las necesidades de TICs de la compañía.
- Disponer de criterios claros para la elaboración y seguimiento de los presupuestos de TIC.
- Contabilizar adecuadamente y de acuerdo con el proceso establecido todos los costos a los servicios asociados a TICs.
- Repercutir los gastos generales de acuerdo con los principios generales de la Organización.
- Los costos asociados al equipamiento, derechos de uso del software, y licencias de uso exclusivo de un área serán sufragados por rubros de los procesos misionales.
- Los costos asociados a este equipamiento, amortización de inversiones y licencias de uso compartido por varias áreas, gastos de alquiler, mantenimientos, entre otros serán imputados proporcionalmente a su uso a cada dirección, según criterios establecidos por la Organización.
- Los costos derivados de la utilización de los sistemas de información que dan servicio a todos los usuarios de la empresa, por ser los soportes de procesos corporativos para la gestión de los diferentes recursos: humanos, comunicaciones, materiales, entre otros; así como aquellos que dan servicio al desarrollo de las actividades directivas de la empresa: planificación, presupuesto, entre otros, serán costeados por el área que ostente la titularidad funcional correspondiente.

Gestión de la configuración: El planteamiento de identificación y control de la configuración deberá estar alineado con la estructura del catálogo de servicios vigente, así como con las directrices de control que se establezcan desde gestión de cambios y de acuerdo con lo establecido por el proceso de gestión de la configuración.

El proceso de gestión de la configuración determinará el nivel de detalle y de profundidad en la definición de los componentes del servicio, manteniendo una base de datos de las configuraciones, en función de la criticidad del servicio relacionado y el valor que aporte mantener la información.

Gestión de cambios: Los pasos deben estar identificados con un número único de cambio.

El área de Tics., aprobará después de analizar los riesgos, el impacto del cambio y el procedimiento de "marcha atrás" en el caso de ser necesario.

No están permitidas las instalaciones ni actualizaciones que no estén bajo el proceso de control de cambios.

Los pasos se llevarán a cabo en horarios cuya afectación a la disponibilidad sea mínima y bajo condiciones controladas (ventanas de cambio).

POLÍTICA DE MANEJO Y PROTECCIÓN DE LA INFORMACIÓN

Todos los colaboradores, consultores, contratistas y terceras partes que manejen información de la empresa, están obligados a salvaguardarla en los sitios dispuestos para tal fin, para garantizar la disponibilidad, confidencialidad y respaldo de la misma.

Estándares de la Política de manejo y protección de la información

Carpetas compartidas: El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información. Por lo tanto, su uso debe ser controlado y para eso se debe evitar el uso de carpetas compartidas en equipos de escritorio.

Los administradores de la red establecen e implementan en los casos aprobados la configuración de acceso a las carpetas, previo requerimiento formal de la misma por medio del comité de gobierno digital.

El usuario que autoriza el acceso a las carpetas y dispone el recurso compartido, es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

Se debe definir el tipo de acceso y los roles estrictamente necesario sobre la carpeta (lectura, escritura, modificación, borrado).

Para la información confidencial o critica para la compañía, deben utilizarse las carpetas destinadas en el servidor de archivos de usuarios, con el fin de que sea incluida en las copias diarias de respaldo.

El acceso a carpetas compartidas debe delimitarse a los usuarios que realmente necesitan la información y se debe proteger el ingreso con contraseñas.

No se puede compartir carpetas o el acceso a carpetas compartidas, a usuarios que no cuenten con software de antivirus corporativo y actualizado (Adquirir antivirus corporativo, PETI).

Respaldo de la información: Las copias de seguridad de la información y de software se deben realizar periódicamente, considerando lo siguiente:

- Establecer registros precisos y completos de las copias de seguridad y procedimientos de recuperación documentados.

- La extensión y frecuencia de las copias de seguridad (totales o incrementales) debe supeditarse a los requisitos de la empresa, legales y de seguridad, respecto a la criticidad de la información.

- Las copias de seguridad deben almacenarse en un lugar diferente y alejado que no esté sujeto a los mismos riesgos de la ubicación principal. Estas deben almacenarse en armarios ignífugos con acceso restringido (PETI).

- La retención de las copias de seguridad será acorde con las tablas de retención definidas en el Sistema de Gestión Documental o en el Sistema de Gestión de Calidad.

Responsabilidad de uso: La Organización pone al servicio de los colaboradores el uso de los medios necesarios para el normal desarrollo de las labores propias del cargo para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta. Es deber de los colaboradores acogerlas con integridad y dar a los recursos uso racional y eficiente.

La Organización, en respeto de los principios de libertad de expresión y privacidad de información, no genera a los colaboradores ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medios electrónicos que sean propiedad de la empresa. En consecuencia, podrá denegar el acceso a los servicios electrónicos, inspeccionar, monitorear y cancelar servicios asignados como correo electrónico, navegación en Internet y recursos compartidos, entre otros.

Los usuarios de los servicios electrónicos aceptan y convienen que la Organización puede conservar y revelar el contenido del correo si así le es requerido por ley o si de buena fe considera que dicha reserva o revelación es necesaria para: (a) cumplir con procesos legales, (b) responder a quejas de que algún contenido viola los derechos de terceras personas, o (c) proteger los derechos, propiedad o seguridad personal de la empresa, sus usuarios y el público en general.

La violación de los controles de seguridad o el incumplimiento de las Políticas de la Organización por parte de los colaboradores dará lugar a la aplicación de medidas administrativas, disciplinarias, civiles o penales a las que haya lugar.

Los estándares de seguridad de la información contienen las políticas de uso aceptable para:

- Correo electrónico.
- Navegación en Internet.
- Recursos compartidos.
- Equipos de cómputo.
- Comunicaciones móviles.
- PLCs.
- Antenas.
- Sensores en general.

POLÍTICA DE RESPONSABILIDAD EN EL USO DE LAS TIC

Todos los colaboradores, consultores, contratistas, terceras partes que utilicen los servicios tecnológicos de telecomunicaciones, información y comunicación, están obligados a cumplir con la Política de TICs, planteada por la Organización.

POLÍTICA DE SOPORTE A LOS USUARIOS DE LAS TIC

El comité de gobierno digital, será el único canal por medio del cual se reportará cualquier incidente o requerimiento asociado a las TIC, con el fin de garantizar el seguimiento y entrega oportuna del servicio solicitado.

Estándares de la Política de soporte a los usuarios de las TIC

Gestión de requerimientos: El área de Tics, garantiza la disponibilidad del comité de gobierno digital como único canal para atender los requerimientos de los usuarios de acuerdo con el catálogo de servicios establecido, para ofrecer una respuesta oportuna y con calidad, con base en los acuerdos de nivel de servicio ofrecidos.

Por medio del correo electrónico institucional, se mantiene informado al usuario de la evolución del requerimiento. Todos los actores que participan en la gestión de requerimientos tienen acceso al correo electrónico con el objetivo de conseguir un buen funcionamiento del proceso. En el caso de que exista riesgo de incumplimiento del Nivel de Servicio, se debe informar al usuario de este hecho.

Atención de incidentes: El área Tics, garantiza la disponibilidad del comité de gobierno digital como único canal para atender los incidentes de los usuarios, de acuerdo con el catálogo de servicios establecido.

Los analistas encargados del tema deben seguir el procedimiento para realizar las actividades de registro, asignación de prioridad, valoración del impacto, clasificación, actualización, escalado, resolución y cierre formal del incidente reportado.

La atención de incidentes debe restaurar el servicio tan pronto como sea posible con la aplicación de una solución temporal o definitiva. Por medio del correo institucional, se mantiene informado al usuario de la evolución del incidente. En el caso que exista riesgo de incumplimiento del Acuerdo de Nivel de Servicio se debe informar al usuario de este hecho.

POLÍTICA DE RELACIÓN CON INFRAESTRUCTURA DE TERCEROS

La infraestructura tecnológica de la Organización que se expone a terceros, debe ser siempre aprobada por el comité de gobierno digital.

POLÍTICA DE GESTIÓN DEL RIESGO TIC

El área de la tecnología la información y las comunicaciones, debe identificar, calificar, priorizar y realizar el tratamiento de los riesgos tecnológicos, con base en los objetivos de la empresa y de acuerdo con la Política de gestión de riesgos corporativa.

POLÍTICA DE INCORPORACIÓN AL CUMPLIMIENTO REGULATORIO

Toda solución de servicios o infraestructura tecnológica debe cumplir con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la Organización.

POLÍTICA DE PROTECCIÓN DEL MEDIOAMBIENTE

El desarrollo de las TIC debe orientarse bajo las estrategias globales de protección del medioambiente y de la Política del Sistema de mejoramiento de la calidad y gestión medioambiental de la Organización, para reducir el impacto medio ambiental en la empresa.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Todos los colaboradores, consultores, contratistas, terceras partes que acceden activos de información de la Organización están en la obligación de continuar protegiendo la información por medio del cumplimiento de las políticas de seguridad, durante y aún después de terminar su relación contractual con la empresa, de acuerdo con lo pactado entre las partes.

DOCUMENTACIÓN RELACIONADA

- Política de Gestión Humana.
- Sistema de Gestión de la Calidad y Gestión Medioambiental de la organización.
- Código de Buen Gobierno Corporativo.
- Política de Seguridad de la Información.

Artículo 2do: La presente Resolución, rige a partir de su expedición.

Dado en la Ciudad de Marinilla a los 16 días del mes de Octubre de 2020.

PUBLÍQUESE Y CÚMPLASE

FELIX HERNANDO GOMEZ RAMIREZ
Gerente

Proyecto: Wilfer Loaiza Orozco
Reviso: