POLÍTICAS Y ESTÁNDARES PARA LA GESTIÓN Y GOBERNABILIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

Establecer un marco de gobierno para que el uso de las TIC's de la empresa logre satisfacer las necesidades actuales y futuras derivadas de la estrategia del negocio, siguiendo los principios de innovación, competitividad, proactividad y seguridad de la información establecidos por el Gobierno Nacional a través de la Política de Gobierno Digital.

2. ALCANCE

Estas políticas son aplicables a todos los colaboradores, consultores, contratistas y terceras partes que usen las tecnologías de información y la comunicación de la empresa.

3. LÍNEA BASE DE LA POLÍTICA

3.1 Responsabilidad

Es responsabilidad la Dirección Administrativa hacer uso de la **Política de Tecnologías de la Información y Comunicación (TIC)** como parte de sus herramientas de gobierno y de gestión, y definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

El Responsable Institucional de dar cumplimiento a la **Política de Gobierno Digital** es el representante legal, quien será además el responsable de coordinar, hacer seguimiento y verificación su implementación. (Decreto 1008 de 2018, Artículo 2.2.9.1.3.2)

3.2 Cumplimiento

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

3.3 Excepciones

Las excepciones a cualquier cumplimiento de **Política de Tecnologías de la Información y Comunicación (TIC)** deben ser aprobadas por la Dirección Administrativa, la cual puede requerir autorización de la Gerencia General de la empresa. Todas las excepciones deben ser formalmente documentadas, registradas y revisadas.

3.4 Administración de las Políticas

Las modificaciones o adiciones de la **Política de Tecnologías de la Información y Comunicación (TIC)** serán propuestas por la Gerencia General de la empresa a través de la Dirección Administrativa. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

4. DESCRIPCIÓN POLÍTICAS Y ESTANDARES

4.1 Adquisición, implementación y mantenimiento de las TIC

Política de Adquisición, Implementación y Mantenimiento de las TIC

La Dirección Administrativa es la responsable de la adquisición, implementación y mantenimiento de todos los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), requeridas para los procesos de la empresa, 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 sistema 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 empresa tienen la responsabilidad de hacer las pruebas necesarias.

Desarrollo de aplicaciones: Las aplicaciones que desarrollen los colaboradores deben cumplir con los requerimientos de seguridad establecidos por la empresa 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 colaboradores dentro de su trabajo será propiedad de la empresa, salvo acuerdo escrito expreso que diga lo contrario.

Los colaboradores o terceros que tengan acceso a los sistemas TIC de la empresa, 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 criptográfico, en caso de utilizarse, 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, el reinicio de los sistemas y los procedimientos de recuperación a utilizar en caso de falla del sistema.

Separación de ambientes: Para minimizar los riesgos en el proceso de puesta en producción de los cambios y nuevos desarrollos, así como el impacto por la no disponibilidad de los servicios, se debe establecer una segregación de ambientes, (Desarrollo, Pruebas y Producción), considerando:

- Definir y documentar las reglas para el paso de software entre ambientes.
- El uso de diferentes equipos, dominios y directorios.
- La restricción de uso de compiladores, editores y otras herramientas de desarrollo o recursos del sistema en ambientes de producción.
- Los sistemas de prueba deben emular al sistema productivo tan real como sea posible.
- El uso de perfiles de usuario diferentes para los diferentes ambientes.
- Los menús deben mostrar mensajes de identificación adecuados para reducir el riesgo de error.
- La restricción de uso de datos de producción en ambientes de prueba. En caso de ser necesario se debe utilizar un mecanismo de enmascaramiento.

Computación en Nube–Cloud Computing: La virtualización de escritorios debe garantizar que todos los datos de usuarios se almacenen de una manera central, y que la información no se almacene a nivel local.

El PU de Sistemas y Tecnología evaluará el impacto y los riesgos en términos de capacidad, disponibilidad, continuidad y seguridad, de las solicitudes de servicios de virtualización, según el proceso de gestión de cambios.

Los proveedores de servicios de virtualización podrán ser utilizados para ambientes de desarrollo y continuidad. Cualquier excepción debe ser autorizada por la Dirección Administrativa, con base en un análisis de riesgos.

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.

Todo medio magnético utilizado que no se requiera debe ser destruido, de manera que no se pueda recuperar la información. En el caso de documentos, estos se deben destruir con las herramientas adecuadas.

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 con soportes debidamente cifrados cuando sean requeridos.

Registros de auditoría: Se deben conservar registros de auditoría de las actividades de los usuarios, incluyendo administradores y operadores, de las excepciones o incidentes de información y mantenerlos durante un período acordado para ayudar en investigaciones futuras y en el seguimiento y monitoreo del control de acceso:

En la medida de lo posible se incluirá como mínimo en los registros:

- Identificadores de usuarios.
- Registro de intentos de acceso al sistema exitosos y rechazados.
- Registro de intentos de acceso a los recursos y a los datos exitosos y rechazados.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de dispositivos y aplicaciones del sistema.
- Archivos a lo que se ha accedido y la clase de acceso.
- Alarmas por el sistema de control de acceso.

- Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión.
- Cambios o intentos de cambios en las posiciones y en los controles de seguridad del sistema.

La frecuencia con que se revisan los resultados de las actividades de seguimiento, dependerá de la información y criticidad de los sistemas.

INFRAESTRUCTURA INFORMÁTICA

Uso de las Redes: la Dirección Administrativa es la responsable de definir las necesidades que tiene la compañía con respecto a las redes. Es responsable también de la administración de los anchos de banda necesarios para soportar los servicios TIC.

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 la Dirección respectiva y seguir los estándares de implementación.

Telefonía: 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 de la Mesa de Ayuda, hacia el proveedor de telecomunicaciones.

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

Telepresencia: La compañía dispondrá de salas de videoconferencia para establecer contacto virtual entre los colaboradores de las diferentes sedes, permitiendo acortar distancias y hacer más eficientes los procesos. Para tal fin se dará uso de las licencias de Google Meet incluidas en el licenciamiento de Google Business.

Radiocomunicación: los servicios de radiocomunicación son de uso exclusivo de las subunidades de operación. Las solicitudes, después de pasar por los niveles de autorización prestablecidos, serán canalizadas por medio de la Mesa de Ayuda hacia el proveedor de telecomunicaciones.

4.2 Equipos portátiles y dispositivos móviles

Política para equipos portátiles y dispositivos móviles

La Dirección Administrativa, a través del PU de Sistemas y Tecnología, 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 empresa.

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. La Dirección Administrativa, 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 consignadas en la Matriz de Atributos y con la aprobación del Director 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.

La Dirección Administrativa, a través del PU de Sistemas y Tecnología, tiene bajo su responsabilidad el suministrar 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.

Los servicios de voz y datos en la telefonía celular, deben ser utilizados por el colaborador exclusivamente para realizar las funciones establecidas para su cargo y su uso debe estar orientado a agilizar las funciones inherentes a su cargo.

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

La Dirección Administrativa revisará 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 serán validados con el Director respectivo y deducidos por nómina si no hay una justificación al respecto.

El colaborador que se retire de la empresa, si desea continuar con la misma línea telefónica, debe solicitarlo por escrito a la Dirección Administrativa para proceder con el trámite de ceder la línea de empresarial a nombre del colaborador, así mismo los planes serán sujetos a las tarifas comerciales del Operador Móvil. El dispositivo debe ser reintegrado a la Dirección Administrativa.

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.

Asimismo, 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 la salud 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 asignará servicio de Internet móvil a los colaboradores que se desplazan fuera de las instalaciones frecuentemente y deben permanecer en lugares donde resulta difícil la comunicación.

Los colaboradores que viajen de manera eventual, deben solicitar el servicio de Internet móvil a través de un requerimiento a la Mesa de Ayuda.

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 la salud de los colaboradores, entre otros

4.3 Gestión de servicios TIC

Política para la gestión de servicios TIC

La Dirección Administrativa promueve la adopción de un enfoque basado en procesos integrados, preservando los principios de arquitectura empresarial, 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, la Dirección Administrativa 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 proceso de Gestión 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:

- Mejorar de manera continua los servicios y los procesos.
- Corregir cualquier falta de conformidad en el servicio o con los planes de gestión.
- 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 empresa, para su posterior seguimiento e implantación.

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

- Disponer de unos presupuestos que sean equilibrados y adecuados con las necesidades de la compañía.
- Disponer de criterios claros para la elaboración y seguimiento de los presupuestos.
- Contabilizar adecuadamente y de acuerdo con el proceso establecido todos los costos de los servicios asociados a TI.
- Repercutir los gastos generales de acuerdo con los principios generales de la empresa.
- Los costos asociados al equipamiento, derechos de uso del software, y licencias de uso exclusivo de un área serán sufragados directamente por la respectiva Dirección.
- 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 Dirección Administrativa.
- 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, documentales, entre otros; así como aquellos que dan servicio al desarrollo de las actividades directivas de la empresa: Planificación, Presupuesto, etc. serán costeados por la Dirección que ostente la titularidad funcional correspondiente.

Gestión de problemas: Todos los problemas deben ser registrados, clasificados, actualizados, escalados, resueltos y cerrados. El procedimiento debe considerar la gestión proactiva de los problemas. En los casos en que para resolver el problema haya que ejecutar un cambio, se realizará según lo establecido por el proceso de Gestión de Cambios.

La gestión de problemas debe ser supervisada y revisada por la Dirección Administrativa, a través del PU de Sistemas y Tecnología. Se deben realizar informes de los problemas gestionados. Esta información debería estar disponible para el proceso de gestión de incidentes de tal manera que se pueda aumentar su efectividad y desempeño.

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 a producción deben estar identificados con un número único de cambio.

El PU de Sistemas y Tecnología en compañía del líder de cada Dirección o la persona asignada para tal fin, aprobarán los pasos a producción después de analizar los riesgos, el impacto del cambio y el procedimiento de "marcha atrás".

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

La frecuencia y el tipo de despliegue se determinará en función de las necesidades y teniendo en cuenta la planificación vigente.

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

Gestión de capacidad: La gestión de capacidad se concreta en un Plan de Capacidad que debe estar alineado con las necesidades de la compañía e incluye:

- Requisitos de capacidad y desempeño, actuales y previstos.
- Plazos, umbrales y costos para las actualizaciones de los servicios.
- Evaluación de los efectos que sobre la capacidad tienen las actualizaciones anticipadas del servicio, peticiones de cambio y nuevas tecnologías.
- El impacto de los cambios regulatorios que afecten la tecnología.
- Los datos y los procesos para poder realizar análisis predictivos.

Se debe monitorear la capacidad del servicio mediante herramientas que analicen los datos de los sistemas. Datos que se traducirán en informes e indicadores, utilizados para conseguir los niveles de capacidad requeridos por la empresa.

Gestión de disponibilidad: Se deben identificar los requisitos de disponibilidad para los servicios, en función de las necesidades de la empresa, los acuerdos de niveles de servicio ofrecidos y las evaluaciones de riesgo. Los requisitos identificados deben incluir aspectos relativos a los tiempos de atención y respuesta, así como la disponibilidad de extremo a extremo de los componentes de los sistemas que soportan el servicio.

Los requisitos se deben registrar en el Plan de Disponibilidad, el cual será revisado por lo menos una vez al año y siempre que se produzcan cambios significativos. Los cambios necesarios para la gestión efectiva de este proceso deben realizarse según el proceso de Gestión de Cambios. El Comité de Cambios conformado por la Gerencia, la Dirección Administrativa y el PU de Sistemas y Tecnología, debe valorar el impacto sobre la disponibilidad de los servicios y el plan de disponibilidad.

Gestión de continuidad: Se deben identificar los requisitos de continuidad para los servicios en función de las necesidades de la empresa, los Acuerdos de Niveles de Servicio ofrecidos y las evaluaciones de riesgo.

Los requisitos se registran en un Plan de Continuidad, el cual será revisado por lo menos una vez al año y siempre que se produzcan cambios significativos. Una vez realizados los cambios se debe probar el plan para comprobar su adecuación y documentar el resultado de las pruebas. En caso que no se alcancen los resultados previstos, se deben establecer acciones encaminadas a su consecución.

Los cambios necesarios para la gestión efectiva de este proceso deben realizarse según el proceso de gestión de cambios. El Comité de Cambios debe valorar el impacto sobre la continuidad de los servicios y el plan de continuidad. Los cambios realizados en producción deben ser actualizados en los planes de continuidad respectivos.

4.4 Manejo y protección de la información

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 de la Mesa de Ayuda.

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). Además, se debe especificar el límite de tiempo durante el cual estará publicada la información y el recurso compartido en el equipo.

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 debe compartir carpetas a usuarios que no cuenten con software de antivirus corporativo y actualizado.

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 negocio, 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.
- 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 Mejoramiento de la Calidad.

Responsabilidad de uso: La empresa 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 empresa, 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 empresa 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 empresa 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 a aceptable para:

- Correo electrónico.
- Navegación en Internet.
- Recursos compartidos.
- Equipos de cómputo.
- Comunicaciones móviles.

4.5 Responsabilidad en el uso de las TIC

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 TIC, planteada por la empresa.

4.6 Soporte a los usuarios de las TIC

Política de responsabilidad en el uso de las TIC

La Mesa de Ayuda 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: La Dirección Administrativa garantiza la disponibilidad de una Mesa de Ayuda, a través del PU de Sistemas y Tecnología, 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 de la herramienta de Mesa de Ayuda se mantiene informado al usuario de la evolución del requerimiento. Todos los actores que participan en la gestión de requerimientos tienen acceso a dicha herramienta 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.

Gestión de incidentes: la Dirección Administrativa, a través del PU de Sistemas y Tecnología, garantiza la disponibilidad de una Mesa de Ayuda 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 Gestión de incidentes debe restaurar el servicio tan pronto como sea posible con la aplicación de una solución temporal o definitiva. Por medio de la herramienta de Gestión del servicio, 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.

4.7 Relación con infraestructura de terceros

Política de relación con infraestructura de terceros

La infraestructura tecnológica de la empresa que se expone a terceros, debe ser siempre aprobada por la Dirección Administrativa, a través del PU de Sistemas y Tecnología.

4.8 Gestión del riesgo TIC

Política de gestión del riesgo TIC

La Dirección Administrativa, a través del PU de Sistemas y Tecnología, debe identificar, calificar, priorizar y realizar el tratamiento de los riesgos tecnológicos, con base en los objetivos de negocio y de acuerdo con la Política de gestión de riesgos corporativa.

4.9 Incorporación al cumplimiento regulatorio

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 empresa.

4.10 Protección del medioambiente

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, para reducir el impacto medio ambiental en la empresa.

4.11 Seguridad y Privacidad de la información

Política de seguridad y privacidad de la información

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

La información sujeta a tratamiento por parte de la empresa, se deberá proteger mediante el uso de las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, claramente detalladas en el Manual de la Política de Datos de la empresa.

No obstante y dando cumplimiento a la Política de Gobierno Digital, la empresa deberá definir un indice de informacion clasificada y reservada, cuyos conjuntos de datos serán publicados en el sitio oficial del Gobierno Nacional establecido para tal fin o través del sitio web oficial de la empresa.

5. 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.
- **Arquitectura empresarial:** Conjunto de elementos organizacionales (estrategia, estructura, procesos más tecnología, personas) que se relacionan entre sí, garantizando la alineación desde los niveles más altos (estratégicos), medios (tácticos), hasta los más bajos (operativos), con el fin de optimizar la generación de productos y servicios que conforman la propuesta de valor entregada a los clientes.
- **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.
- **Datos Abiertos:** son información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales para su aprovechamiento. En Colombia, la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública Nacional, define los datos abiertos en el numeral sexto como "*todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos*".
- **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 una entidad autorizada.
- **Empresa:** Se refiere a Empresas Públicas de la Ceja E.S.P. o EEPP de La Ceja E.S.P.

- **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 entrega los servicios de tecnología.
- **Políticas:** Toda intención y directriz expresada formalmente por la administración de la Organización.
- **Procesos:** Se define un proceso de negocio 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 su objeto de negocio.
- **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 (accountability), no repudio y fiabilidad.
- **TIC:** Se refiere a las Tecnologías de Información y las Comunicaciones
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.