EMPRESAS MUNICIPALES DE CALI

EMCALI E.I.C.E E.S.P.

RESOLUCION No. GG- 0 0 1 5 1 7 DE 24 JUN 2014

(Por medio de la cual EMCALI E.I.C.E. – ESP Adopta las Políticas de Seguridad de la Información)

El Gerente General de las Empresas Municipales de Cali EMCALI EICE ESP., Nombrado por el Señor Alcalde de Santiago de Cali, mediante Decreto No. 411.020.0606 del 19 de Septiembre del 2013, en uso de sus facultades legales y

CONSIDERANDO

Que EMCALI EICE E.S.P. mediante Resolución No.1548 de Octubre 20 de 2011, ha reconocido la importancia de la información, y en general de los activos de información para el cumplimiento de los objetivos estratégicos de la empresa y la continuidad de la operación, adoptando el Sistema de Gestión de Seguridad de la Información.

Que mediante Resolución No. 0164 de 2014, se complementó la estructura organizacional del SGSI desde el Nivel Estratégico, Táctico y Operativo.

Que el Sistema de Gestión de Seguridad de la Información de EMCALI está basado en la Norma ISO/IEC 27001 la cual es totalmente integrable con los Sistemas de Gestión de Calidad ISO 9001 y otros Sistemas implementados en la empresa.

Que la Norma ISO/IEC 27001 es un estándar desarrollado por la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission), que proporciona el modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en un ciclo de PHVA (Planear-Hacer-Verificar-Actuar) de mejora continua, utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Que la seguridad de la información permite proteger los activos de información contra una amplia gama de amenazas, asegurando así la continuidad del negocio,

reduciendo al mínimo el daño de los activos y maximizando el retorno de inversión y las oportunidades de negocio.

Que la confidencialidad, la integridad, la disponibilidad y la trazabilidad de la información son características con las que deben contar los activos de información, y que se consideran esenciales para asegurar que la información sea accesible únicamente a los usuarios debidamente autorizados, que se prevenga el acceso no autorizado voluntario o accidental a la información, que se garantice la salvaguardia de la completitud y exactitud de la información y sus métodos de procesamiento y el establecimiento de su ubicación y estado a través de los procesos, lo que es necesarios para lograr los objetivos de la organización y el desarrollo de las funciones de los usuarios cuando, lo requieran.

Que es necesario aumentar el nivel de conciencia en Seguridad de la Información en las Empresas Municipales de Cali EMCALI EICE ESP, articulando el entorno tecnológico y organizacional, dentro del marco normativo y regulatorio local e internacional.
Que los sistemas de información de la organización están expuestos a un número cada vez más elevado de amenazas, que podrían aprovechar las vulnerabilidades existentes para someter los activos de información que se encuentren en riesgo crítico, a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Que se requiere la implementación de las Políticas de Seguridad de la Información para que sean la base del cumplimiento legal al interior de la Organización, de modo que permita brindar la protección adecuada de los activos de EMCALI y se apoye activamente al logro de los objetivos estratégicos del negocio.

Que las Políticas de seguridad de la información fueron aprobadas en Comité de Gerencia General, sesionando como Comité de Seguridad de la Información el día lunes 12 de mayo de 2014, lo cual consta en el acta de la misma reunión.

RESUELVE

ARTÍCULO PRIMERO: Implantar las Políticas de Seguridad de la Información que son la base legal para el Sistema de Gestión de Seguridad de la Información (SGSI) en EMCALI EICE E.S.P., bajo los parámetros aplicables de la Norma ISO/IEC 27001:2013 y el Código de Buenas Prácticas en Gestión de la Seguridad de la Información ISO/IEC 27002.

ARTÍCULO SEGUNDO: Las Políticas de Seguridad de la Información aprobadas en el comité del SGSI de acuerdo a cada dominio son:

1. **Dominio: Política de Seguridad de la Información**

EMCALI E.I.C.E. E.S.P. como empresa líder en la prestación de servicios públicos domiciliarios, de tecnologías de la información y las comunicaciones, y actividades complementarias, se compromete en:

Mantener los criterios de Confidencialidad, Integridad, Disponibilidad y Trazabilidad de la información, para incrementar los niveles de competitividad, rentabilidad y sostenibilidad, alineados con la normatividad vigente y el direccionamiento estratégico de la Organización.

Establecer y documentar los controles, procedimientos y normas de seguridad, los cuales deben ser de estricto cumplimiento por todos los servidores públicos y terceros, que tienen acceso a la información de la Organización.

Fomentar entre los grupos de interés, la adopción y cumplimiento de las políticas, controles, procedimientos y normas de seguridad de la Información en EMCALI E.I.C.E. E.S.P.

Aplicar las normas establecidas cuando un servidor público o un tercero infringen las Políticas de Seguridad de la Información.

Contribuir con la transparencia, legalidad, agilidad, calidad y continuidad de los servicios.

2. **Dominio: Organización de Seguridad de la Información**

EMCALI E.I.C.E. E.S.P. estructura y verifica que las responsabilidades para la gestión de la seguridad de los activos de información están claramente separadas y asignadas en los diferentes niveles organizacionales, incluyendo el Comité de Seguridad de la Información.

Las responsabilidades de los diferentes roles y la asignación de los mismos está definida mediante resolución interna.

3. **Dominio: Seguridad de los Recursos Humanos**

EMCALI E.I.C.E. E.S.P. establece la responsabilidad del funcionario por el manejo seguro y adecuado dado a los activos de información, la cual se extiende aun después de finalizada la relación laboral o contractual; así mismo garantiza el entendimiento de lo anterior, mediante la debida instrucción, socialización y suscripción de acuerdos de confidencialidad. Esto se hace extensivo a aquellos

contratistas y terceros que tengan acceso a la información de EMCALI E.I.C.E. E.S.P.

4. Dominio: Gestión de Activos de Información

Los activos de información de EMCALI E.I.C.E. E.S.P. son inventariados, asignados a un responsable y clasificados de acuerdo con los criterios y requerimientos del Sistema de Gestión de Seguridad de la Información. De acuerdo con la clasificación, se establecen los niveles de protección, responsabilidad, el nivel de acceso y los procedimientos para su manipulación, los cuales se revisan periódicamente y cuando se presentan cambios en los activos de información.

5. Dominio: Control de Acceso

EMCALI E.I.C.E. E.S.P. establece las medidas de control de acceso a nivel de red, sistema operativo, aplicaciones y acceso físico que garantice la eficiencia, eficacia y efectividad del sistema, de acuerdo con el tratamiento correspondiente al nivel de clasificación de cada activo. EMCALI E.I.C.E. E.S.P. se reserva el derecho de monitoreo a fin de identificar de manera inequívoca cada usuario y el uso debido de los sistemas de información.

6. Dominio: Criptografía

EMCALI E.I.C.E. E.S.P. utiliza para la protección de los activos de información, claves y aplicaciones criptográficas basadas en normas de construcción internacionales ampliamente probados y recomendados por asociaciones de reconocida trayectoria, e igualmente fomenta su uso para todas las situaciones y comunicaciones que involucren datos sensibles y demás que considere relevante.

EMCALI E.I.C.E. E.S.P. dispone de los recursos y elementos técnicos requeridos para entrenar a sus usuarios en la construcción de claves fuertes, así como para cubrir todas las necesidades de encriptación que han sido evaluadas y aprobadas como tal por el Comité Técnico de Seguridad de la Información, previa recomendación y estudio técnico.

7. Dominio: Seguridad Física y Ambiental

Las dependencias organizacionales cuentan con protecciones físicas y ambientales acordes con la clasificación de los activos que protegen, incluyendo áreas seguras para la gestión, almacenamiento y procesamiento de información, perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas adecuados de

contención, detección y extinción de incendios, que preservan el medio ambiente.
Se garantizan los protocolos de Seguridad de la Información en condiciones de mantenimiento, traslado, eliminación o cuando la información o los equipos se den de baja.

Todo medio de almacenamiento o centro de procesamiento de terceros, que procese o almacene información de EMCALI E.I.C.E. E.S.P. debe cumplir con la seguridad física y tecnológica requerida con el propósito de mantener la disponibilidad, integridad, confidencialidad y trazabilidad de la información requerida por el negocio.

8. Dominio: Seguridad de las Operaciones

Los procedimientos y responsabilidades de administración y seguridad pertinentes a cada ambiente tecnológico están documentados, de forma que garantice una debida gestión de cambios, el seguimiento a los estándares de seguridad definidos y la atención de incidentes de seguridad que se presenten.

Los roles y responsabilidades de las áreas y/o procesos están debidamente diferenciadas para reducir las oportunidades de modificación a los activos de información. La planificación y aprobación de los sistemas de información son adecuados y consideran las necesidades futuras de la empresa.

EMCALI E.I.C.E. E.S.P. asegura el mantenimiento, administración y custodia de los activos de información, al igual que la seguridad en el intercambio de información, mediante controles que garanticen su confidencialidad, integridad, disponibilidad y trazabilidad, así mismo provee protección contra software malicioso.

Las condiciones y niveles de servicio de los contratos que se realizan con proveedores, soportan los Acuerdos de Niveles de Servicio (ANS) y tienen indicadores que permiten medir su calidad y cumplimiento.

El proceso de Gestión de TI, adelantado por la Gerencia de Tecnologías de la Información (GTI) o quien haga sus veces, debe asegurar que sus servicios estén disponibles y funcionen correctamente siempre que los clientes y usuarios deseen hacer uso de éstos en el marco de los ANS firmados con ellos.

9. Dominio: Seguridad de las Comunicaciones

El proceso de Gestión de TI adelantado por la GTI o quien haga sus veces, debe segmentar y categorizar las redes para reducir los riesgos de modificación y uso no autorizado de los activos de información, garantizando que la planificación y aprobación de los sistemas de información son adecuados y consideran las

necesidades futuras.

Se implementan protecciones para la transferencia de información, entre otras, acuerdos de confidencialidad y no divulgación, políticas de transferencia de información y controles sobre los mensajes electrónicos.

10. Dominio: Adquisición, Desarrollo y Mantenimiento de Sistemas

EMCALI E.I.C.E. E.S.P. hace un debido análisis e implementación de los requerimientos de seguridad de los sistemas de información internos y/o adquiridos, que incluye garantías de validación de usuarios, datos de entrada y salida, y del procesamiento de los mismos, de acuerdo con la clasificación de los activos a tratar en el sistema.

Los responsables de la información deben considerar los requerimientos de seguridad necesarios para mantener la integridad y confidencialidad, en una etapa temprana del ciclo de desarrollo de sistemas, así mismo son responsables de la incorporación de los controles relevantes en el nuevo sistema.

El responsable de la Seguridad de la Información, debe verificar los resultados de las pruebas realizadas para evitar poner en riesgo la organización. Esta regla incluye a los sistemas que reciben modificaciones significativas, como nuevos desarrollos.

11.Dominio: Relaciones con los Proveedores

EMCALI E.I.C.E. E.S.P. realiza un debido proceso de selección y evaluación de los proveedores en su cadena de suministros y realiza los correspondientes acuerdos que garantizan la protección requerida de la información compartida durante la relación contractual, incluso luego de terminada dicha relación.

Todas las modificaciones y ajustes a los contratos son igualmente verificados para continuar entregando los niveles adecuados de protección a la información de EMCALI E.I.C.E. E.S.P.

12. Dominio: Gestión de Incidentes de Seguridad de la Información

EMCALI E.I.C.E. E.S.P. promueve la debida gestión a los incidentes de Seguridad de la Información, siguiendo procedimientos apropiados para su atención, manejo y evaluación del impacto causado al negocio.

Todos los funcionarios, contratistas y demás personal interno o externo que tenga un vínculo contractual con EMCALI E.I.C.E. E.S.P., debe reportar como incidente de

seguridad cualquier anomalía o mal uso de los activos de información de EMCALI E.I.C.E. E.S.P., según el instructivo de atención de incidentes establecido.

13.Dominio: Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio

Se evalúa el impacto de eventos que afectan los procesos de EMCALI E.I.C.E. E.S.P. y se realizan planes de continuidad en aquellos que son críticos para su operación y supervivencia.

Los planes de continuidad deben considerar medidas técnicas, administrativas y de vínculo con instituciones externas. Los planes se deben probar y revisar periódicamente y están articulados en toda la empresa con recursos tecnológicos y no tecnológicos.

14. Dominio: Cumplimiento Legal

EMCALI E.I.C.E. E.S.P. cumple con los requisitos legales internos y externos aplicables a la Seguridad de la Información que gestiona. Incluye entre otras los derechos de propiedad intelectual, la protección de datos personales, los tiempos de retención de registros, la privacidad de información, el uso debido de recursos de procesamiento, el uso de criptografía y la recolección de evidencia y auditorías.

EMCALI E.I.C.E. E.S.P. garantizará que todo el software instalado en la organización cumple con la ley de derechos de autor y la normatividad vigente (Ley 23 de 1982 y Ley 44 de 1993), Ley de Derechos de Autor.

15.Incumplimiento y Sanciones

Si una persona natural o jurídica viola las disposiciones de la política de Seguridad de la Información, por omisión, por extralimitación o intencionalmente, EMCALI E.I.C.E. E.S.P. tomará las medidas correspondientes, de conformidad con la legislación vigente en materia de responsabilidad civil, penal, administrativa y disciplinaria, en especial de las normas contenidas en Reglamento Interno de trabajo de EMCALI E.I.C.E. E.S.P. y Ley 734 de 2002."

ARTÍCULO TERCERO: El Comité Técnico deberá definir los mecanismos que le permitan medir la efectividad y aplicación de las Políticas e informar periódicamente al Comité del SGSI (Comité de Gerencia General) el avance y resultados de la gestión del SGSI.

ARTÍCULO CUARTO: Evaluación de metas: Corresponde a la Dirección de Control Interno DCI de EMCALI EICE ESP, la revisión del cumplimiento de los planes, metas,

objetivos, indicadores y factores críticos de éxito, con el fin de propender el cumplimiento de las Políticas de Seguridad de la Información.

ARTÍCULO QUINTO: Modificaciones: Los ajustes o modificaciones a las Políticas de Seguridad de la Información de EMCALI EICE ESP sólo podrán realizarse por las siguientes circunstancias:

- Por cambios en la Norma ISO/IEC27001:2013
- Por cambios en la Estructura Organizacional o la legislación que impacten a las Políticas
- Por solicitud de los Entes de Control del Estado, previa auditoría
- Por auditoría realizada por el Ente Certificador.
- Por recomendación del Comité Técnico del SGSI

ARTÍCULO SEXTO: Vigencia: La presente Resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

OSCAR ARMANDO PARDO ARAGON
Gerente General de EMCALI EICE ESP

Proyectó: Luz Stella Mora-GTI
Revisó: Edison Carvajal – Abogado contratista, Alba Luz Pantoja -Coordinadora Área Funcional Control de Legalidad
Aprobó: Nicolás Orejuela Botero -Secretario General – Jairo Trujillo – Gerente GTI