Emsercota S.A.

EMPRESA DE SERVICIOS PÚBLICOS

MANUAL DE POLITICAS DE SEGURIRAD Y PRIVACIDAD DE LA INFORMACION

2025

TABLA DE CONTENIDO

5.2. REVISIÓN POR LA DIRECCIÓN

1. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

1.1. OBJETIVO DEL MSPI

Establecer las normas, políticas y recomendaciones inherentes a la seguridad y privacidad de la información y al uso de los recursos tecnológicos de la empresa de servicios públicos domiciliarios EMSERCOTA S.A. E.S.P., con el ánimo de preservar los activos de información en óptimos niveles de integridad privacidad y confidencialidad.

1.2. DETERMINACIÓN DEL ALCANCE DEL MSPI

Este manual debe aplicarse para servir a la alta dirección en la protección de los activos, la protección de la infraestructura tecnológica que soporta la operación de la Entidad y gestión de los riesgos de seguridad y privacidad de información. Las políticas aquí enmarcadas deben ser cumplidas por todo el personal de la Entidad sus funcionarios, contratistas, terceros y la ciudadanía en general que accede a la información de la empresa de servicios públicos domiciliarios EMSERCOTA S.A. E.S.P.

2. LIDERAZGO

2.1. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Líder de Seguridad de la Información: Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Comité de Seguridad, realizando la implementación y seguimiento de estos.

- Líder o responsable de protección de datos personales: Establecer lineamientos para la protección de los datos personales tratados en la Entidad.

- Comité Institucional de Gestión y Desempeño: Comunicar a los funcionarios, contratistas y particulares que participan en actividades de forma directa o indirecta con la Entidad, la importancia de satisfacer los requisitos de seguridad digital.

- Líderes de proceso: Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados.

3. POLÍTICAS

3.1. Política de dispositivos móviles

La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad, para lo cual se establecen las siguientes directrices:

- Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.
- Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.
- Es responsabilidad del servidor públicos al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los servidores públicos deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.
- Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la Entidad para el proceso de análisis, evaluación y tratamiento.
- Los dispositivos móviles que son autorizados para salir de las instalaciones por la Entidad deben ser protegidos mediante el uso e implementación de los controles apropiados como: cifrado de

información, políticas de restricción en la ejecución de aplicaciones y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

- Todos los dispositivos móviles propiedad de la Entidad pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.
- Evitar almacenar información de la Entidad que no sea estrictamente necesaria para el desarrollo del trabajo en el dispositivo móvil.
- Cifrar la información confidencial y eliminarla del dispositivo móvil una vez se haga la actividad que corresponda de acuerdo al desarrollo del trabajo.
- Mantener el registro actualizado de los dispositivos móviles de la empresa de servicios públicos domiciliarios EMSERCOTA S.A. E.S.P., asignados a los colaboradores, así como el registro de la instalación del software y hardware requerido por el colaborador.
- Para los dispositivos móviles asignados por la Entidad, se debe notificar al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.
- Evitar la exposición del dispositivo móvil a altas temperaturas.
- Al utilizar el dispositivo móvil en lugares públicos se recomienda mantenerlo siempre vigilado, utilizar guaya de seguridad y en caso de robo o pérdida del equipo notificar a los jefes de las áreas responsables para la realización del debido proceso.
- Desactivar en los dispositivos móviles la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sea necesario.

3.2. Política de Teletrabajo

La Entidad brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza teletrabajos, y se hace uso de los recursos tecnológicos y activos de información autorizados por la Entidad para el desarrollo de las actividades de Teletrabajo, para lo cual se establecen las siguientes directrices:

- Toda información gestionada por la empresa de servicios públicos domiciliarios EMSERCOTA S.A. E.S.P., y que sea accedida remotamente

debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

- EMSERCOTA S.A. E.S.P., establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- La Entidad establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.
- La Entidad revisa la seguridad física y del entorno del sitio donde se va a teletrabajar, con el fin de proteger la confidencialidad, integridad y disponibilidad.
- Al utilizar el dispositivo móvil en lugares públicos se recomienda mantenerlo siempre vigilado, utilizar guaya de seguridad y en caso de robo o pérdida del equipo notificar a los jefes de las áreas responsables para la realización del debido proceso.
- En los lugares que se realiza teletrabajo se debe aplicar las mismas políticas de uso de los activos de información, aplicación de contraseñas, bloqueo de sesión y demás que se relacionen, y en caso sospechar de un evento o incidente de seguridad, informar inmediatamente al área responsable.

3.3. Políticas de Seguridad de los Recursos Humanos

EMSERCOTA S.A. E.S.P., establece directrices para asegurarse que los colaborares y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información, para lo cual se establecen las siguientes directrices:

- La Entidad establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad y privacidad de la información.
- Los acuerdos contractuales entre la Entidad y los servidores públicos o contratistas deben especificar el cumplimiento a los lineamientos de seguridad y privacidad de la información establecida en la Entidad.

- Todos los funcionarios y contratistas deben firmar un acuerdo de confidencialidad y no divulgación, donde se especifiquen la responsabilidad con el acceso y gestión de la información confidencial, de datos personales, derechos de autor, entre otra que tenga implicaciones legales.
- Se debe especificar en los contratos las sanciones que conlleva el uso indebido de la información de la Entidad y Comunicar a los funcionarios y contratistas las obligaciones que deben cumplir con la información de la Entidad al finalizar el contrato o relación laboral.
- El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los Colaboradores o Terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

3.4. Políticas de Gestión de Activos

EMSERCOTA S.A. E.S.P., debe desarrollar estrategias de trabajo para optimizar el uso de los recursos de seguridad, establecer los métodos de identificación clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades y manteniendo mecanismos acordes par el control de riesgos de la información, para lo cual se establecen las siguientes directrices:

- Cada activo de información de la Entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y requerimientos legales de retención.
- La Entidad debe establecer los niveles de clasificación de la información de acuerdo a la normatividad Legal Colombiana y brindar protección a la información de acuerdo con su importancia para la organización.
- Es responsabilidad del líder de proceso, jefe de área o Director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.
- Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

- Se deber solicitar autorización para retirar los medios de la Entidad (USB, portátiles, discos duros etc.) y se debería llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría.
- Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.
- Se debe almacenar la información en la nube autorizada por la Entidad y realizar la configuración técnica que se requiera para obtener la trazabilidad de con quien se comparte la información, fechas y demás datos de interés.

3.5. Políticas gestión de medios de almacenamiento

EMSERCOTA S.A. E.S.P., debe disponer de diferentes mecanismos de almacenamiento para propender por la disponibilidad de la información y el establecimiento de medidas para el control de riesgos de la información. Es importante tener en cuenta que almacenar la información en un sitio centralizado evita duplicidades y problemas de versiones, evita pérdidas de documentos, centraliza las copias de seguridad y facilita compartir información para realizar trabajo colaborativo, para lo cual se establecen las siguientes directrices:

3.5.1. Almacenamiento en la red corporativa

- Para que los colaboradores puedan compartir información única y exclusivamente laborar se dispone de servidores de almacenamiento en red.
- Los controles de acceso a esta información son definidos por el área solicitante de la creación del recurso compartido en la red (carpeta) y el responsable de sistemas, con el objetivo de limitar quién puede acceder, a dónde y los permisos autorizados (lectura, escritura o lectura y escritura)
- Se debe establecer los criterios de almacenamiento corporativos (qué se puede almacenar, quién tiene acceso y cuándo se elimina la información).
- Se debe informar a los empleados sobre la necesidad de cumplir la política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa.
- Se debe Establecer e implementar reglas de acceso que permitan llevar un control de quién tiene acceso y a qué discos/directorios.

- Se debe definir un plan de copias de seguridad en el que se detalla la información a guardar, cada cuanto tiempo se va a realizar, donde se va a almacenar y el tiempo de conservación de la copia.
- Se debe proponer una estructura para el almacenamiento clasificado, es decir creas carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde.
- Se debe realizar auditorías de servidores, que comprenda la revisión periódica del estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.
- Se debe cifrar la información crítica almacenada en los servidores.

3.5.2. Almacenamiento en la nube

- Se debe informar a los colaborares cuales son los servicios de almacenamiento cloud permitidos.
- Se debe informar a los colaboradores los pasos a seguir para un adecuado borrado de la información contenida en los repositorios en la nube.

3.5.3. Almacenamiento en dispositivos extraíbles

- Para los dispositivos de almacenamiento extraíble (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) que guarden información de Entidad, deben aplicársele medidas de seguridad, puesto que son susceptibles al robo, manipulación, extravío e infección por virus.
- La Entidad autoriza el uso de dispositivos de almacenamiento extraíble para el almacenamiento de información de trabajo en caso que sea estrictamente necesario realizar tal acción, además, se debe guardar los activos con clave o cifrado.
- La Entidad no autoriza el uso de dispositivos de almacenamiento extraíble para el almacenamiento de información de trabajo en caso que sea estrictamente necesario realizar tal acción, se debe solicitar autorización por parte del jefe del área.
- Se debe bloquear los puertos USB a todos los equipos de cómputo de la Entidad.

- Si se necesita almacenar información sensible o confidencial en dispositivos externos corporativos, estos deben estar debidamente protegidos por parte del usuario responsable del guardado de esta información, el cual se debe almacenar en lugares seguros y si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.) debe informar inmediatamente al personal encargado de la gestión de incidentes.

3.5.4. Almacenamiento en equipos de trabajo

- A los colaboradores de la Entidad y algunos contratistas se les asigna como herramienta equipos informáticos: ordenadores, tabletas, teléfonos móviles, etc., para el desempeño de sus funciones. Por lo anterior la Entidad debe establecer las directrices para el almacenamiento de manera local en los equipos.
- Se puede guardar información de la Entidad en el disco local del equipo de cómputo asignado, cuando sea estrictamente necesario y no se cuente con otro medio de almacenamiento autorizado ya sean nube o en los servidores de la red.
- No se autoriza el guardado de información en los equipos de cómputo asignados, solo se debe alojar en los recursos autorizados.
- La información que se guarda en los discos locales de los equipos de cómputo de los dispositivos móviles no cuenta con respaldo de información. Para respaldar la información y mantener su conservación por un tiempo determinado por la Entidad, se debe transferirá a los servidores o nube autorizada.

3.6. Políticas Seguridad Física y del Entorno

La Entidad debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización, para lo cual se establecen las siguientes directrices:

- Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Entidad, por tanto, se deben establecer y mantener controles para resguardar la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas, y demás que procesen información.

- Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: a) Al momento de retirar un equipo en la organización (almacén), el proceso de TI realiza una copia de respaldo de la información almacenada en este activo. b. El proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.
- Los servidores públicos y contratistas, garantizan que no se disponga información de la Entidad en los escritorios de los equipos y que esta no estará almacenada y fácilmente copiada o accedida por alguien sin autorización desde un computador desatendido.
- Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.
- Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de la Entidad.
- Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

3.7. Políticas de Controles Criptográficos

La debe asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información, para lo cual se establecen las siguientes directrices:

- Se deben utilizar técnicas criptográficas y cifradas como son: Para la transferencia o almacenamiento de información sensible o pública reservada se debe cifrar asignando clave para abrir el archivo.
- Los discos duros internos, externos y memorias USB utilizados por las diferentes áreas o procesos de la Entidad, están cifrados mediante algoritmos de cifrado simétrico. El personal de cada proceso es quien

debe solicitar el cifrado de la información que esté clasificada como crítica o sensible por la Entidad.

- La Entidad asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información. Por lo cual establece técnicas criptográficas y cifradas como son: Cifrado de la información cuando se requiere trasferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado.
- El acceso remoto a la red y los sistemas de información de la Entidad desde una red externa, será a través de conexiones seguras.
- Se debe contar con buenas prácticas para la gestión de llaves.

3.8. Políticas Seguridad en las Operaciones

EMSERCOTA S.A. E.S.P., debe propender porque las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información, se brinde protección contra código malicioso, gestión de vulnerabilidades, respaldo de información entre otros, que son necesarios para asegurar la correcta operación de los procesos técnicos y la protección de la información, para lo cual se establecen las siguientes directrices:

- La Entidad garantiza que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información.
- Los cambios en la Entidad deben ser tratados a través, de un procedimiento establecido de gestión de cambios con el fin de minimizar los riesgos de alteración de los sistemas de información.
- Según la clasificación de la información establecida por la Entidad, se deben establecer las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento o en la nube.
- Los responsables de TI definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.
- El proceso de TI es el encargado de aplicar los parches, controles o remediaciones derivadas de la ejecución de pruebas periódicas de análisis de vulnerabilidades.

- Se debe Realizar un listado del software existente autorizado en la Entidad y diseñarle el plan de actualización y aplicación de parches de seguridad, para esto se debe tener en cuenta la revisión de características y los requisitos de las actualizaciones y parches del fabricante antes de instalarlos.
- Se debe implementar mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente.

3.9. Políticas Seguridad de las Comunicaciones

La Entidad debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte, para lo cual se establecen las siguientes directrices:

- Se debe implementar tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red como por ejemplo un firewall de seguridad perimetral.
- El Proceso de TI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.
- El proceso de TI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.
- Se debe aplicar un método para gestionar la seguridad de las redes dividiéndola en dominios de red separados, por ejemplo: Red de dominio de acceso público y red de dominio de computador de escritorio, dominio de servidor), junto con unidades organizacionales (por ejemplo, recursos humanos, finanzas, mercadeo) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples unidades organizacionales). La separación se puede hacer usando diferentes redes físicas o diferentes redes lógicas (por ejemplo, redes privadas virtuales).
- Se debe evitar dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, o almacenados incorrectamente como resultado de una marcación incorrecta.

- La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.
- La Entidad asegura la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.

3.10. Políticas Adquisición, Desarrollo y Mantenimiento de Sistemas

La Entidad debe propender porque la Seguridad de la Información sea parte integral de los sistemas de información dentro ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presten servicios a la Entidad, para lo cual se establecen las siguientes directrices:

- Se debe establecer el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.
- La Entidad garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.
- La Entidad asegura que se diseñe e implemente 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 Entidad debe establecer controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.
- La Entidad cuenta con un ambiente de desarrollo y de pruebas seguro o, en su defecto, exige al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes.

- Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.
- La Entidad debe establecer una metodología de desarrollo seguro de software.

3.11. Políticas de Gestión de Incidentes de Seguridad

EMSERCOTA S.A. E.S.P., debe asegurarse que todos los colaboradores conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información, para lo cual se establecen las siguientes directrices:

- Se debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.
- Todos los servidores públicos y contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información
- 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 o comunicar a un ente competente para que realice el debido proceso.
- La Entidad establece y ejecuta 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.
- La Entidad debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.
- La Entidad debe establecer y poner a disposición de los colaborados el formato o mecanismos de reporte de eventos e incidentes de seguridad y privacidad de la información.
- La Entidad debe contar con una bitácora de los incidentes de seguridad de la información reportados y atendidos y el establecimiento de indicadores relacionados a la gestión de los incidentes de seguridad y privacidad de la información.

3.12. Políticas Cumplimiento

- La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente, para lo cual se establecen las siguientes directrices:
- Se debe analizar los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos y brindar los lineamientos que permitan dar cumplimiento a la normatividad legal.
- La Entidad asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.
- La Entidad, debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

4. APOYO O SOPORTE

4.1. TOMA DE CONCIENCIA

Brindar lineamientos para que los servidores públicos, contratistas y proveedores de la Entidad reciban la educación y formación en toma de conciencia adecuada, y actualizaciones sobre las políticas y procedimientos.

Le proceso de Gestión de Talento Humano y el supervisor del contrato, deberán velar por que los servidores públicos, contratistas y proveedores de la Entidad, que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.

Será responsabilidad de Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

4.2. COMUNICACIÓN

La Entidad deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son:

Correo Electrónico, intranet y comunicaciones impresas.

El presente manual de políticas de Seguridad y Privacidad de la Información, será comunicado a todas las partes interesadas de la Entidad, a través de las tecnologías de la información y medios físicos de ser necesario.

Todas las políticas, procedimientos y demás documentos relacionados con la seguridad y privacidad de la información serán publicados en la página web de la entidad, Será responsabilidad de Recursos Humanos, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

La periodicidad para el desarrollo de actividades está establecida en el plan de concientización de seguridad y privacidad de seguridad determinado anualmente.

5. EVALUACIÓN DEL DESEMPEÑO

5.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

EMSERCOTA S.A. E.S.P., debe asegurar que la seguridad y privacidad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales, para lo cual se establecen las siguientes directrices:

- Seguimiento de tareas, actividades o acciones asignadas en reuniones de comités donde se traten los temas de seguridad y privacidad de la información.
- Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y demás normas de seguridad y privacidad de la información.
- Generación de Informe de resultados de las revisiones del Modelo de Seguridad de la Información al interior de los procesos.

- Seguimiento y presentación de los resultados del último ciclo de auditoría interna al MSPI (informe de Auditoría Interna).
- Realizar los cambios en las cuestiones internas y externas que sean pertinentes al MSPI.
- Analizar propuestas o mejoras al MSPI por parte de los servidores públicos y contratistas.
- Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para Seguridad y privacidad de la Información sólo aplica las acciones correctivas y de mejora.
- Gestionar obtener la realimentación de las partes interesadas, respecto a la implementación de seguridad y privacidad de la información.
- Gestionar, analizar y documentar los resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos.
- Identificar las vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Revisión y actualización anual en caso que aplique de la política general, la revisión de las políticas específicas de seguridad, de objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

5.2. REVISIÓN POR LA DIRECCIÓN

La dirección tiene que revisar el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Entidad, de la empresa a intervalos planificados, ya que se tiene que asegurar la idoneidad, la adecuación, la eficiencia y la alineación continuas con los objetivos estratégicos de la Entidad, la revisión por la dirección tiene que planificarse y realizarse una vez al año el análisis de los resultados de la Evaluación y Desempeño.

ANA AIDA PARDO CARRILLO
Subgerente Corporativo

YAMIR GEOVANNY QUEVEDO AGUDELO
Técnico Administrativo Sistemas

Proyecto: Yamir Geovanny Quevedo Agudelo – Técnico Administrativo sistemas