PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca
Sede Administrativa Calle 26 51-53. Torre Beneficencia Piso 3.
Bogotá, D.C. Tel. 749 1535 - 749 1541

/ElCundinamarca @InmobCund
contactenos@eic.gov.co www.eic.gov.co

Tabla de Contenido

Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca
Sede Administrativa Calle 26 51-53. Torre Beneficencia Piso 3.
Bogotá, D.C. Tel. 749 1535 - 749 1541
/EICundinamarca @InmobCund
contactenos@eic.gov.co www.eic.gov.co

- **Introducción**

Actualmente en el desarrollo de actividades que se tiene al interior de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, se ha venido evidenciando la importancia que se debe focalizar a los procesos de tecnología y la seguridad que estos requieren, con el fin de prestar y mantener un servicio adecuado, es por eso que día a día es necesario sumar capacidades y esfuerzos para conservar y preservar de manera adecuada y segura toda la información que se recibe, genera, resguarda o manipula desde los ámbitos corporativos especialmente en el sector público, debido a la importancia que se le da a la clasificación a la información por parte de personas que se dedican a validar los niveles de seguridad de las entidades públicas. Este último con un crecimiento alto debido a la situación que actualmente se afronta por la pandemia mundial de Covid-19, mediante la cual las personas se debieron reguardar en sus casas, y donde las entidades tanto públicas como privadas se han visto forzadas a realizar o implementar la modalidad de teletrabajo, dejando expuestas vulnerabilidades a nivel de seguridad en las infraestructuras tecnológicas.

Con base a lo anterior, se ha visto la necesidad de realizar inversiones de recursos para fortalecer las capacidades técnicas, profesionales y de infraestructura, con el fin de garantizar la continuidad de los servicios ofertado y asegurar la integridad de la información y sistemas en los que se operan.

- **Objetivo General**

Establecer lineamientos, directrices, procesos y procedimientos con el fin de salvaguardar la integridad y seguridad de la información que se opera en la entidad.

- **Objetivos Específicos**

a) Establecer acuerdos de servicio con sustentos de seguridad que permita la prestación de servicios a la ciudadanía y entidades públicas y privadas de manera continua e ininterrumpida.
b) Establecer medios de apropiación para la apropiación y uso de la Política de Seguridad que se encuentra vigente para los funcionarios y contratistas.
c) Disminuir las brechas de seguridad de acuerdo a las pautas establecidas por el Ministerio de Tics.
d) Definir políticas las cuales estén orientadas al fortalecimiento de normatividad y prevención frente a la seguridad informática de los procesos y procedimiento que se desarrollan en la entidad.
e) Fortalecer el equipo profesional y la infraestructura tecnológica de la entidad con el fin de disminuir los riesgos que se puedan materializar en la ejecución de actividades de la entidad.

- **Alcance**

La finalidad que se espera lograr con la estructuración de este documento, es mejorar la estrategia frente a la prevención de parámetros de seguridad, enfocados al manejo y adecuado análisis, planeación, estructuración, implementación, monitoreo y control de los proyectos que se gestionen desde la entidad y en pro de fortalecer la estructura funcional.
Los cuales tendrán el objetivo de optimizar los sistemas de información y optimizar los canales de comunicación que se encuentran establecidos en la EIC, permitiendo un mayor nivel de participación, integración, percepción, uso y apropiación tanto a nivel interno como externo, conforme a lo establecido en los dominios del marco de referencia del Ministerio de Tecnologías de la Información y

Telecomunicaciones, en cumplimiento y apoyados en el Plan Estratégico para la vigencia (2020-2023), facilitando la integración de las dependencias y garantizando el adecuado servicio a la comunidad y entidades.

La gestión y el tratamiento de los riesgos de seguridad de la información se aplicará, a través de la aplicación de principios básicos y metodológicos para la administración de la información, así como técnicas, actividades y buenas prácticas que contribuyan a la toma de decisiones para la prevención de incidentes al interior de la Entidad.

- **Política de Seguridad y Privacidad de la Información**

Las políticas de seguridad de la información que se estructuran o se proyectan en la entidad tienen como finalidad identificar, generar un plan de acción, mitigación, tercerización u omisión de los riesgos de seguridad informática de los sistemas de información o infraestructura tecnológica que se tenga en la entidad, lo que garantice el adecuado cumplimiento de los objetivos estratégicos, operativo y misionales de la EIC.

La información en la EIC es un recurso que se categoriza como un activo de valor el cual debe ser protegido de toda amenaza presente, por esto es que es importante que los principios de integridad y seguridad de la información sean parte fundamental de la cultura organizacional de la entidad. Por tal razón, el compromiso de las directivas de la entidad y sus área de apoyo en la estructuración, consolidación, difusión y cumplimiento de los lineamientos establecidos en esta política.

- **Lineamientos**

a) Preservar los recursos de información y gestión de la EIC, de los cuales hagan uso de la infraestructura tecnológica con la que cuenta la entidad y sea utilizada para su procesamiento, en cuanto a las amenazas, internas o externas identificadas, deliberadas o accidentales, cada una de estas con un plan de contingencia con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
b) Garantizar la adopción e implementación de los lineamientos de seguridad que se establezcan en esta política, actualizaciones y/o generación de nuevos documentos, analizando los requerimientos funcionales, económicos y profesionales necesarios para el cumplimiento de la política.
c) Preservar la Política de Seguridad de la EIC actualizada, con la finalidad de brindar los lineamientos necesarios que se deban tener en cuenta durante la vigencia del Plan Estratégico de la EIC.

- **Alcance**

Esta política se deberá aplicar en toda la estructura organizacional de la EIC, dando cobertura y seguridad sobre los procesos, procedimientos, recursos físicos, personal interno y externo con los que cuente la entidad.

- **Nivel de cumplimiento**

Todos los funcionarios internos, externos, entidades vinculadas, proveedores y en general todos los participantes identificados y mencionados en el alcance de la misma, deberán cumplir con la política definida.

Con base en lo anterior, se procede a establecer políticas que soportes y den respaldo al Plan de Seguridad y Privacidad de la Información de la EIC

a) Se deberá realizar la implementación de un sistema de gestión de seguridad de la información con el fin de dar cobertura a los lineamientos establecidos los cuales estén alineados a la necesidad de la entidad y a los requerimientos tecnológicos que se definan por el Min Tic.
b) Los deberes y responsabilidades frente a la seguridad de la información deberán ser definidas, socializadas, publicadas, apropiadas y aceptadas por todos los involucrados en el flujo de información (empleados, funcionarios, contratistas, proveedores, terceros y/o entidades).
c) La EIC será la única unidad organizacional encargada de realizar la protección de la información generada, procesada, recibida, resguardad y en general de todo tipo de clasificación que se manejen en los procesos y activos de información que hacen parte de la entidad.
d) La EIC es la única que tiene la potestad de proteger la información y garantizar su integridad y disponibilidad idónea con el fin de minimizar impactos de índole financiero, operativo o legal, debido al mal uso, afectación por malware, robo o cualquier otro tipo de riesgo.
e) La EIC es la única autorizada para realizar modificación o acceder a los sistemas de información o instalaciones en las cuales se encuentren los equipos de tecnología mediante los cuales se procesa o maneja la información.
f) Los funcionarios internos o externos deberán aceptar todos los procesos o procedimientos que se establezcan en la entidad, con el fin de dar cumplimiento a los lineamientos de seguridad de la información.
g) La información que se reciba por entidades, interesados o ciudadanos en general, deberá ser verificada y monitoreada por la entidad y sus funcionarios a cargo.
h) La disponibilidad de la información estará a cargo de la entidad según los parámetros correspondientes y establecidos por su área de Tics.
i) Todos los procesos y procedimientos focalizados al cumplimiento de los criterios de seguridad de la información establecidos por la EIC, deberán estar alineados conforme a lo que se encuentra definido en la Ley 1581 de 2012 y las demás normas que tengan relación o definían alguna normatividad.

Cada una de las responsabilidades definidas en la política de seguridad y privacidad de información, deberá tener una responsabilidad legal y normativa aplicable a cada una de los responsables de incumplimiento a estas, incluyendo lo que establezca la normatividad a nivel departamental y nacional sobre el tema en mención.

- **Normatividad pertinente**

..1. Normatividad que se deberá definir según la estructura organizacional de la seguridad de la información.

- Normas dirigidas a la Gerencia:
  - La Gerencia deberá definir y establecer los roles y responsabilidades de acuerdo a los lineamientos de la seguridad y privacidad de la información en los niveles directivos y operativos.
  - Se deberá establecer el procedimiento idóneo ante la materialización de cualquier riesgo externo a la entidad y su oportuno comunicado con las autoridades responsables.
  - La Gerencia será la encargada de realizar la verificación y aprobación de las políticas de seguridad y privacidad de la información, estructuradas en este documento y demás que respalden el proceso.
  - La Gerencia será la encarga de definir las estrategias o asignar responsabilidades necesarias para fomentar la cultura organizacional necesaria para el entendimiento de la política.
  - La Gerencia deberá establecer los canales de divulgación de las políticas de seguridad y privacidad de la información a todos los funcionarios de entidad.
- Normas dirigidas a la Gerencia y Subgerencia:
  - En cabeza de estas dependencias se deberá realizar la asignación de recursos necesarios para cubrir la demanda de infraestructura tecnológica y personal de apoyo, técnico o profesional que sea necesario para cubrir las necesidades de la EIC.
  - Se deberá estructurar un comité de seguridad interno, el cual tenga una integración con lo definido o estructurado a nivel central, con el fin de aunar esfuerzos y responsabilidades frente a la seguridad de la información de la Gobernación de Cundinamarca.
- Normas dirigidas al Comité de seguridad de la información
  - Será el encargado de realizar la proyección, actualización, modificación de las políticas aplicables a la entidad y las cuales deberán presentarse a la Junta Directiva de la EIC.
  - Presentar ante la Junta Directiva la metodología aplicable para el plan de tratamiento de riesgos de seguridad de la información.
  - Presentar ante la Junta Directiva el plan de clasificación de información según la importancia de la información generada.
  - El Comité deberá asumir responsabilidad sobre los incidentes de seguridad que le sea asignados, activando el plan de tratamiento de riesgos y haciendo contacto con las autoridades responsables cuando sea necesario.
  - Deberá apoyar a la Gerencia con la verificación y seguimiento al cumplimiento de las políticas establecidas en la entidad.
- Normas dirigidas al Área de tics
  - Será la encargada de liderar todos los procesos y procedimientos para la gestión de la parte de TI en la EIC.

- Establecer políticas, procesos y procedimientos para la gestión de seguridad y privacidad de la información.
- Establecer controles necesarios desde la parte técnica, física, administrativa y lógica para afrontar las vulnerabilidades identificadas.
- Realizar el apoyo a la Gerencia frente a la asignación de roles, responsabilidades y funciones a los funcionarios de la EIC con el fin de cubrir todos los aspecto a nivel de seguridad y privacidad de la información e integridad de la infraestructura tecnológica.

- Normas dirigidas a la Oficina de Control Interno
  - Será la responsable de planificar, estructurar, ejecutar, monitorear y controlar las auditorías frente a los sistemas de gestión de información con los que cuente la EIC.
  - Realizar la verificación de los procesos, procedimientos políticas, estándares, metodologías o cualquier tipo de documento que se genere desde el área de tics.
  - Validar la integridad de la documentación generada por el área de tics, frente a los requerimientos de orden departamental o nacional.
  - Garantizar la revisión de forma parcial o total de los procesos y procedimientos que están focalizados al cierre de brechas de seguridad y privacidad de la información.
  - Generar un informe de seguimiento y control sobre las auditorías realizadas o los hallazgos que se deriven de las mismas.
- Normas dirigidas a todos los Usuarios (funcionarios, contratistas, proveedores, entidades, ciudadanos)
  - Deberán acoger y aceptar todos los lineamientos, políticas y demás normatividad o responsabilidades definidas por la EIC, a fin de dar cumplimiento a todos los estándares de seguridad necesarios para garantizar el adecuado funcionamiento de la entidad.

..2. Normatividad para uso de conexiones remotas

- Normas dirigidas al Área de tics
  - Se deberán establecer procedimientos y procesos documentados los cuales soporten de manera técnica los métodos de conexión remota a la plataforma con la que cuenta la EIC.
  - Se deberán garantizar los respaldos de seguridad idóneos para ejecutar las conexiones remotas, y tener una trazabilidad y registro de cada dispositivo, usuarios y niveles de seguridad para cada conexión.
  - Se deberán tener las restricciones de seguridad adecuadas para garantizar que el acceso remoto a los equipos o infraestructura tecnológica de la EIC, sea realizado por únicamente por personal autorizado.
  - Se deberán realizar pruebas de conexión mediante las cuales se verifiquen los procesos y procedimientos establecidos por la EIC.
  - Garantizar la integridad, seguridad y licenciamiento si aplica de las herramientas utilizadas para soportar las conexiones remotas a los equipos.
- Normas dirigidas a la Oficina de Control Interno
  - Se deberá realizar la auditoría frente a los procesos establecidos para las conexiones remotas, con el fin de garantizar los niveles de seguridad idóneos para la EIC.

- Normas dirigidas a todos los Usuarios (funcionarios, contratistas, proveedores, entidades, ciudadanos)
    - Las conexiones que se realizan deberán estar respaldados por software de seguridad o antivirus, con el fin de generar un puente de comunicación estable y seguro.
    - Aceptar las condiciones o políticas establecidas por la EIC, con el fin de disminuir los riesgos de seguridad que se puedan presentar.
    - Se deberán realizar las conexiones remotas desde terminales que se encuentren debidamente registradas e identificadas por el área de tics, con el fin de disminuir los riesgos de seguridad.

..3. Normatividad relacionada con la vinculación de funcionarios

- Normas dirigidas a la Subgerencia – Personal talento humano
    - Se deberá realizar la verificación correspondiente de la información anexada por el personal que se encuentra postulado para la vinculación con la EIC.
    - Garantizar la estructuración de un documento de acuerdo y/o cláusula de confidencialidad, el cual deberá ser socializado, aceptado y firmado por los nuevos integrantes de la EIC.
    - Socializar y dar a conocer los procesos y procedimientos frente las políticas que se tienen establecidas en la EIC.
- Normas dirigidas a Supervisores y Directivos
    - Se deberá realizar la verificación del documento de acuerdo y/o cláusula de confidencialidad en el proceso contractual del personal, antes de realizar la asignación de tareas o información a manejar.

..4. Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios.

- Normas dirigidas a la Subgerencia – Personal talento humano
    - El apoyo de talento humano deberá realizar el proceso de desvinculación, vacaciones o cambio de funciones de acuerdo a lo establecido por la EIC.
    - Realizar el correspondiente informe para el área de tics, con el fin de realizar las actividades correspondientes frente al uso y manejo de la información.
- Normas dirigidas a Supervisores y Directivos
    - Se deberá informar de manera inmediata al área de tics frente a cualquier desvinculación o cambio de labores del personal que se encuentra a cargo de los mencionados.
- Normas dirigidas al Área de tics
    - Se deberá realizar la desvinculación y verificación de información asignada o generada por el usuario con el fin de garantizar su integridad.
    - Realizar el respaldo idóneo de la información encontrada de los usuarios que se reportan para desvinculación.

..5. Normas de responsabilidad por los activos de información

- Normas dirigidas a los Propietarios de los activos de información
  - Los directivos y supervisores de contratos o de funcionarios deberán actuar como los responsables y propietarios de la información tanto a nivel físico o digital, lo que los faculta en propiedad para permitir o restringir el acceso a la información de acuerdo a los parámetros establecidos.
  - Los propietarios de los activos de información deberán generar un inventario de todos los recursos con lo que cuenta y realizar la actualización correspondiente a medida que sea necesario.
  - Los propietarios de la información deberán realizar el seguimiento de los permisos de accesos a la información digital y de forma física garantizar que el manejo sea únicamente realizado por personal autorizado.
  - Deberán garantizar la integridad de la información y disponibilidad correcta frente a los procesos de auditoría que se requieran o ejerzan en la EIC.
- Normas dirigidas al Área de tics
  - Será el responsable de la propiedad, manejo, integridad y disponibilidad de la información que se genere de manera virtual, por consiguiente deberá garantizar la adecuada seguridad de la misma.
  - En conjunto con el Comité de seguridad, serán los responsables de autorizar la instalación, cambio, modificaciones, parametrizaciones o eliminación de componentes que estructuren la plataforma de tecnología de la EIC.
  - Serán los responsables de realizar la entrega, recepción, soporte o verificación de los activos físicos de tecnología que hagan entrega u asignación a funcionarios de la EIC.
  - Realizar los respectivos respaldos de información de los activos de información digital cuando se realicen cambios de funciones, retiro del cargo, vacaciones o cualquier acción que requiera garantizar el respaldo de la información.
  - Se deberá realizar una identificación de riesgo de manera periódica para estar actualizando la matriz de riesgo y los planes de acción frente a estos.
  - Monitorear constantemente la infraestructura y los recursos de la plataforma con el fin de subsanar posibles fallas.
- Normas dirigidas a los Directivos
  - Se deberá autorizar el uso de los medios dispuestos por el área de tics por los funcionarios que integran cada uno de sus equipos.
  - Deberán recibir los elementos, equipos, información y demás activos, los cuales sean entregados por los funcionarios cuando terminen actividades, tengan vacaciones, cambio de funciones o retiro del cargo.

- **Inventario de Activos de Información**

La EMPRESA INMOBILIRIA Y DE SERVICIOS LOGÍSTICOS DE CUNDINAMARCA deberá establecer procesos y procedimientos, mediante los cuales le permita obtener un conocimiento claro y exacto sobre los activos que posee como parte importante de la administración de riesgos.

Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems, impresoras, servidores), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para LA EMPRESA INMOBILIARIA Y DE SERVICIOS LOGÍSTICOS DE CUNDINAMARCA.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas

las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

- **Plan de Comunicaciones**

..1. Introducción

En la última década, las tecnologías de información y comunicaciones (TIC) se han convertido en las herramientas por excelencia para la optimización de los procesos y el funcionamiento eficaz de una empresa o entidad.

Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad e integridad de la información que se encuentra disponible en las diferentes plataformas, afectando de esta manera el desempeño normal de la entidad.

Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

..2. Objetivo general

Generar una cultura de tecnología en los cargos directivos, la cual permita que se tenga un nivel de apropiación idónea para afrontar la importancia de trabajar activamente en el proceso de implementación de los controles de seguridad de la información, propiciando su compromiso, la toma de conciencia y su responsabilidad respecto al mismo, su sostenibilidad y continuidad.

..2.1. Objetivos específicos

- Establecer la temática y forma para realizar capacitaciones en seguridad de la información.
- Construir material para sensibilización y difusión focalizada a la prevención.
- Lograr que cada funcionario conozca sus roles y responsabilidades de seguridad y privacidad de la información dentro de la EIC.
- Crear una cultura de integridad, confidencialidad y disponibilidad de la información donde todos los miembros de la entidad comprendan la importancia de dar un tratamiento adecuado a la información.
- Evaluar, medir y cuantificar, si el programa implementado genero impacto en el desarrollo de las actividades de la Entidad.
- Mantener informados a los funcionarios, contratistas o terceros sobre las nuevas

vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática.

..3. Descripción general del plan de sensibilización, comunicación y capacitación

El plan de sensibilización, comunicación y capacitación, es un programa efectivo que busca que todos los funcionarios de la EIC cumplan las políticas de seguridad de la información mediante actividades, capacitaciones, talleres y socializaciones.

¿POR QUÉ NECESITAMOS UN PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN?

Existe la mentalidad que no hay nada importante por proteger en su computador.

Se tiene el concepto errado que la tecnología por si misma puede resolver los problemas de seguridad.

Continuamente se generan nuevos métodos mediante engaños que buscan obtener información confidencial.

Deben conocer tanto las amenazas externas como las internas.

Debido a las anteriores razones, el plan de sensibilización, comunicación y capacitación será diseñado e implementado para seguir los requerimientos exigidos por Gobierno en Línea, logrando que los funcionarios conozcan los motivos y razones que generan los diferentes tipos de incidentes en seguridad de la información que existen alrededor de cada uno y acojan las debidas precauciones recomendadas a través de las diferentes actividades de concienciación y sensibilización.

..4. Diseño del plan de sensibilización, comunicación y capacitación

La gran mayoría de las personas, desconoce sobre temas de seguridad de la información y en especial, el alcance del tema. Es muy común encontrar que en las empresas el personal confunde seguridad informática con seguridad de la información, así como otros están convencidos que la información es solo la documentación digital desconociendo que también lo es la documentación impresa. La mayoría de las vulnerabilidades provienen desde el interior de las propias empresas (empleados descontentos, fraude interno, accesos no autorizados, poca motivación, carencia de entrenamiento organizacional y desconocimientos de las políticas de seguridad).

Es muy fácil adquirir las contraseñas de un usuario en la red de la entidad, de sus correos electrónicos y es muy fácil vulnerar los sistemas de seguridad y cifrado. En los puestos de trabajo se pueden encontrar contraseñas escritas en las agendas, pegadas en la pantalla o debajo del teclado.

Las alternativas que se recomiendan utilizar para que el plan de sensibilización, comunicación y capacitación sea factible son:

1. Folletos
2. Afiches
3. Letreros
4. Fondos de Pantalla
5. Uso de correo institucional
6. Capacitaciones y socializaciones con los temas correspondientes a la seguridad de la información.

La campaña de sensibilización a los diferentes grupos objetivo definidos, tendrá una duración mínima de 12 meses, que iniciarán con el plan de sensibilización, comunicación y capacitación, apoyo por medio de los afiches y folletos para dar a conocer masivamente la campaña para todo el personal de la entidad.

Algunos de los aspectos que se deben tratar en este plan de sensibilización, comunicación y capacitación:

1. Uso de contraseñas.
2. Protección contra los virus.
3. Respetar la política de seguridad.
4. Instrucciones al uso del correo electrónico.
5. Buen uso de internet.
6. Backup de la información.
7. Pasos a seguir en caso de incidentes.
8. Ingeniería social.
9. Seguridad para los dispositivos USB.
10. Indicar medidas se seguridad para el envío de información sensible o confidencial.
11. Software permitido y no permitido.
12. Seguridad de los equipos.

Elaborado por:	**Nombre:** German Darío Landinez González **Cargo:** Contratista – Profesional Universitario
Revisado por:	**Nombre:** **Cargo:**
Aprobado por:	**Nombre:** **Cargo**