Contenido

1. POLITICA DE CONFIDENCIALIDAD DE LA INFORMACION

RESUMEN. La Dirección de Tránsito de Bucaramanga se compromete a proteger la información confidencial que se encuentra bajo su control. Esta política establece los requisitos bajo los cuales cada uno de los miembros de la entidad debe tratar la información (pública, interna y reservada), protegiéndola de su divulgación no autorizada a terceros, garantizando su confidencialidad y estableciendo las responsabilidades del personal de planta y contratistas para el cumplimiento de esta normatividad.

Se considera información confidencial:

- Información de la Dirección de Tránsito de Bucaramanga declarada como confidencial e información entregada por terceros bajo un acuerdo de confidencialidad.
- Datos de empleados, contratistas o terceros relacionados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que no hayan sido difundidos públicamente.
- Documentación relacionada con las actividades de las distintas áreas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que no haya sido difundida públicamente por la misma.

INTRODUCCION. La confidencialidad es la seguridad de que la información será protegida y no divulgada sin la aprobación del propietario de dicha información. La información que la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA declare como confidencial se regirá por un conjunto de reglas que limiten el acceso a la información.

ALCANCE. Esta política es aplicable a empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA y se refiere a las acciones individuales o conjuntas realizadas por o en nombre de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO. Establecer reglas que permitan la protección de los datos que tiene, maneja y disponen El Personal de Planta y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

Recomendaciones Para garantizar la confidencialidad de la información, se implementan los siguientes mecanismos de control:

- Control de accesos físicos y lógicos para evitar accesos no autorizados.
- Cifrado de datos sensibles en reposo y en tránsito.
- Uso de autenticación multifactor para el acceso a sistemas críticos.
- Auditorías y monitoreo continuo de accesos y manipulación de información.
- Políticas de contraseñas seguras y renovación periódica.

- Capacitación constante al personal sobre buenas prácticas en seguridad de la información.
- Restricción del uso de dispositivos extraíbles para el almacenamiento de información confidencial.

PRINCIPIOS

La DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA ha adoptado un sistema de clasificación de la información que categoriza la información en tres grupos de acuerdo con su grado de confidencialidad.

- Toda la información bajo control de DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, sea ésta generada interna o externamente, se encuentra en una de estas categorías: **Público, Interno y Reservado.**
- Todo el personal de planta y contratistas deben familiarizarse con las definiciones para estas categorías y cumplir con las medidas de protección establecidas para ellas.
- Si la información no está clasificada como pública, ésta no podrá ser proporcionada a ninguna entidad externa sin un acuerdo de confidencialidad.

- El Personal de Planta, contratistas y terceros que trabajan para de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, en ausencia de instrucciones claras o precisas considerarán la información como de uso interno exclusivamente. Esta política aplica especialmente cuando, por algún motivo, no se ha realizado una clasificación de la información.

- Toda la información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA (Pública, Interna y Reservada) debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento.

- Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a empresas no autorizadas, el Propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad informática de la entidad con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.

- No se revelarán los controles de seguridad de los sistemas de información y la forma en que están implementados. Esto incluye: Información que se proporciona en presentaciones, discusiones, o es tratada en diferentes foros que incluya aspectos técnicos de infraestructura.

- Toda información clasificada debe ser etiquetada (marcada) con base en estándares definidos. Se buscará que estas etiquetas sean mantenidas en buen estado y visibles de tal forma que se puede identificar la clasificación de la información de la entidad en cualquier momento.

- Toda la documentación impresa, escrita a mano o documento legible que contenga información clasificada como confidencial o de uso interno, debe tener una etiqueta que indique el nivel apropiado de sensibilidad con base en la clasificación.

RESPONSABILIDADES

Empleados, contratistas y terceros que tengan vínculo con la de DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES

- Garantizar el tratamiento adecuado de la información según su clasificación (pública, interna y reservada).
- Implementar controles adicionales de seguridad debido a la migración de datos y software misional a una plataforma de terceros.
- Asegurar el cumplimiento de normativas de protección de datos y privacidad en el manejo de la información confidencial.
- Fortalecer las responsabilidades del personal de planta y contratistas en la gestión de la información.
- Mejorar la integridad y disponibilidad de la información mediante el uso de tecnologías seguras y auditables.

2. POLÍTICA DE SEGURIDAD DE EQUIPOS MOVILES

RESUMEN. El presente documento define los lineamientos necesarios para el uso dispositivos móviles personales o institucionales que acceden a información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA. Implementando controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la

información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

INTRODUCCION. Los equipos móviles propiedad de la Dirección de Tránsito de Bucaramanga utilizados dentro o fuera de la entidad y en funciones propias de la entidad, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la Dirección de Tránsito de Bucaramanga y deben ser sujetos a un grado equivalente de protección al de los equipos que se encuentran dentro de las instalaciones de la Dirección de Tránsito de Bucaramanga.

ALCANCE. Esta política aplica para todo el personal de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que accedan a información de la entidad a través de dispositivos móviles, y para el personal encargado de configurar de manera segura los dispositivos móviles.

OBJETIVO. Establecer condiciones para uso de equipos móviles personales o institucionales que manejen información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

- Para aquellos dispositivos que no son entregados por parte de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, deben recibir correo de la persona que envió solicitud a Tecnología "**aceptando el cumplimiento la política de dispositivos móviles, así como las configuraciones de seguridad establecidas"**.
- Las computadoras personales deben garantizar en las conexiones a Internet u otras redes deben mantener instalado y actualizado el antivirus.
- Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano.
- Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les deben proporcionar una forma apropiada de protección al acceso, ej. Contraseñas de encendido, inscripción, etc.).
- Con el fin de prevenir acceso no autorizado deben autorizar la instalación de programas o herramientas que permitan proteger datos e información de robos y mantener una protección de datos reactiva para encontrar, bloquear y proteger tus móviles y computadores.
- Proteger los equipos contra la exposición de campos electromagnéticos muy fuertes.
- Los equipos de cómputo de la Dirección de Tránsito de Bucaramanga, así como la información almacenada en los mismos, son propiedad de la Dirección de Tránsito de Bucaramanga, y pueden ser inspeccionados, o utilizados de cualquier manera y en cualquier momento en que la entidad lo considere.
- Los equipos propiedad de la Dirección de Tránsito de Bucaramanga deben ser devueltos a la entidad en el momento en que el usuario deje de tener relación laboral con la entidad.
- Los equipos personales como equipos portátiles, teléfono inteligente o cualquier otro sistema de cómputo usado para actividades de la entidad que contenga información sensible, deberán protegerse y garantizar a través de acuerdos de Confidencialidad la información contenida en estos y el funcionario deberá asumir la responsabilidad sobre el uso y manejo de la información.

- De común acuerdo, los funcionarios podrán solicitar la autorización a la dependencia competente o en su defecto al jefe inmediato el uso del dispositivo móvil, aceptando el cumplimiento de la política de dispositivos móviles y las políticas que apliquen para el uso y manejo de la información, por medio de correo electrónico.
- Los equipos Propiedad de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, serán configurados y estas configuraciones no podrán modificarse mientras se acceda o almacenen información.
- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
- Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
- Para Dispositivos móviles propios de la entidad se debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
- Es necesario realizar el cifrado del dispositivo móvil para dispositivos que tengan criticidad en la información.
- Está prohibido almacenar información personal en los dispositivos móviles asignados por la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.
- En los Dispositivos y Equipos propiedad de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, está prohibido realizar instalación de aplicaciones no autorizadas por la Gestión Técnica o jefe inmediato.
- Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.
- Configurar sólo las cuentas organizacionales en los dispositivos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que tendrán acceso a la información de la Entidad.
- En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, se debe reportar la perdida a la Oficina de las TIC lo más pronto posible.
- En cualquier momento el equipo de Seguridad de la Información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.
- Las Auditorías internas o de tercera parte pueden realizar la verificación de las configuraciones de los equipos móviles y su cumplimiento con los lineamientos de esta política.
- El incumplimiento de esta política traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

RESPONSABILIDAD

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES

- Dar cumplimiento a los lineamientos de la política de seguridad de equipos móviles.
- Garantizar el tratamiento adecuado de la información según su clasificación (pública, interna y reservada).
- Implementar controles adicionales de seguridad debido a la migración de datos y software misional a una plataforma de terceros.
- Asegurar el cumplimiento de normativas de protección de datos y privacidad en el manejo de la información confidencial.
- Fortalecer las responsabilidades del personal de planta y contratistas en la gestión de la información.
- Mejorar la integridad y disponibilidad de la información mediante el uso de tecnologías seguras y auditables.

3. POLITICA DE RETENCION Y ARCHIVO DE DATOS

RESUMEN. Esta política establece el periodo de retención requerido para categorías específicas de datos y establece los lineamientos mínimos a seguir cuando se destruya información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

INTRODUCCION. Es importante definir claramente el tiempo necesario que la entidad debe tener datos específicos, ya que esto ocupa espacio de almacenamiento innecesario y así se eliminan datos irrelevantes identificando los requisitos legales que regulan la retención de datos y si hay información que se debe conservar un tiempo prolongado; se adecua un correcto sistema de archivo de datos administrando la actualización del ciclo de vida de este.

ALCANCE Esta política se aplica a empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA al igual que toda la información física o digital que se use de la entidad.

OBJETIVO Establecer lineamientos que permitan un correcto proceso de retención de datos y adecuado almacenamiento de los datos en los archivos.

PRINCIPIO

El delegado de protección de datos determina el periodo de tiempo para el cual los documentos y registros electrónicos deben ser retenidos mediante el programa de retención de datos. Como excepción, los periodos de retención dentro del programa de retención de datos pueden prolongarse en casos como:

- Las investigaciones en curso de las autoridades de los estados miembros, si existe la posibilidad de registros de datos personales necesarios para la Entidad para demostrar el cumplimiento de los requisitos legales;
- En el ejercicio de los derechos legales en los casos de demandas o procedimientos judiciales similares reconocidos por la legislación local.

Se considerará la posibilidad de que los medios utilizados para el archivo de datos se desgasten. Si se eligen medios de almacenamiento electrónicos, también se almacenarán los procedimientos y sistemas que garanticen que se pueda acceder a la información durante el período de retención (tanto con respecto al soporte de información como a la legibilidad de formatos) para proteger la información contra pérdidas como resultado de futuros cambios tecnológicos. La responsabilidad del almacenamiento recae en el Responsable de Seguridad.

El Personal de Planta y contratistas deben revisar periódicamente todos los datos, ya sea en formato electrónico en su dispositivo o en papel, para decidir si destruyen o eliminan cualquier dato una vez que el fin para el que se crearon esos documentos ya no sea pertinente. La responsabilidad general de la destrucción de datos recae sobre el Responsable de Seguridad.

Una vez tomada la decisión de llevar a cabo la eliminación de acuerdo con el Programa de retención, los datos deben eliminarse, triturarse o destruirse en un grado equivalente al del valor dado por los demás y su nivel de confidencialidad. El método de eliminación varía y depende de la naturaleza del documento. Por ejemplo, cualquier documento que contenga información sensible o confidencial (y, en particular, datos personales sensibles) debe ser eliminado como residuo confidencial y estar sujeto a una eliminación electrónica segura; algunos contratos que han expirado o han sido reemplazados sólo pueden garantizar la trituración interna.

El empleado o contratista deberá realizar las tareas y asumir las responsabilidades pertinentes para la destrucción de la información de manera adecuada. El proceso específico de eliminación o destrucción puede ser llevado a cabo tanto por un empleado o por un proveedor de servicios interno o externo que el Responsable de Seguridad subcontrata para este propósito. Se cumplirán todas las disposiciones generales aplicables según las leyes de protección de datos pertinentes y la política de protección de datos personales de la Empresa.

Deben existir controles adecuados que impidan la pérdida permanente de información esencial de la empresa como resultado de la destrucción intencionada o no intencionada de la información– estos controles se definen en Políticas de Seguridad de la Información.

El Responsable de Seguridad documentará y aprobará por completo el proceso de destrucción. Los requisitos legales aplicables para la destrucción de información, en particular los requisitos de las leyes de protección de datos aplicables deberán observarse plenamente.

La persona designada con la responsabilidad de Protección de datos (el Responsable de Seguridad) tiene la responsabilidad de garantizar que cada una de las oficinas de la Compañía cumpla con esta Política. También es responsabilidad del Responsable de Seguridad ayudar a cualquier oficina local con las consultas de cualquier autoridad de protección de datos local o gubernamental.
Cualquier sospecha de incumplimiento de esta Política debe informarse de inmediato a el Responsable de Seguridad. Se investigarán todas las instancias de supuestas infracciones de la Política y se tomarán medidas según corresponda.

El incumplimiento de esta Política puede tener consecuencias negativas, que incluyen, entre otras, la pérdida de confianza del cliente, litigios y pérdida de ventajas competitivas, pérdidas financieras y daños a la reputación, lesiones personales, daños o pérdidas de la Entidad. El incumplimiento de esta política por parte de empleados permanentes, temporales o contratados, o de terceros, a los que se haya otorgado acceso a las instalaciones o a la información de la Entidad, puede dar como resultado procedimientos disciplinarios o el cese de su empleo o contrato. Tal incumplimiento también puede conducir a acciones legales contra las partes involucradas en tales actividades.

Los registros que pueden destruirse de manera rutinaria a menos que estén sujetos a una investigación legal o reglamentaria en curso son los siguientes:

- Anuncios y avisos de reuniones diarias y otros eventos que incluyen aceptaciones y disculpas;
- Solicitud de información ordinaria como las direcciones de viajes; Reservas para reuniones internas sin cargos/costes externos;
- Documentos de comunicación como cartas, portadas de fax, mensajes de correo electrónico, hojas de ruta, hojas de felicitaciones y elementos similares que acompañan a los documentos pero que no agregan ningún valor; Hojas con mensajes; Lista de direcciones reemplazada, listas de distribución, etc.;
- Documentos duplicados tales como copias CC y FYI, borradores sin cambios, impresiones de instantáneas o extractos de bases de datos y archivos diarios; Publicaciones internas almacenadas que están obsoletas o reemplazadas; y
- Revistas comerciales, catálogos de proveedores, folletos y boletines de vendedores u otras organizaciones externas.

En todos los casos, la eliminación está sujeta a los requisitos de comunicación que puedan existir en el contexto de un litigio.

Los documentos de nivel I son aquellos que contienen información que es de la más alta seguridad y confidencialidad y aquellos que incluyen cualquier dato personal. Estos documentos se eliminarán como residuos confidenciales (triturado de corte transversal e incinerado) y estarán sujetos a eliminación electrónica segura. La eliminación de los documentos debe incluir una prueba de destrucción.

Los documentos de nivel II son documentos privados que contienen información confidencial, como los nombres, firmas y direcciones de las partes, o que podrían ser utilizados por terceros para cometer fraudes, pero que no contienen ningún dato personal. Los documentos deben ser cortados transversalmente y luego colocados en contenedores de basura cerrados para su recolección por una empresa de eliminación aprobada, y los documentos electrónicos estarán sujetos a eliminación electrónica segura.
Los documentos que no contienen información confidencial o datos personales y son documentos publicados de la Entidad. Estos deben ser triturados en tiras o eliminados a través de una empresa de reciclaje e incluir, entre otras cosas, anuncios, catálogos, folletos y boletines informativos. Estos pueden ser eliminados sin una pista de auditoría.

Recomendaciones sobre la Gestión de Activos de Información

- **Protección de activos de información:** Los activos de información se protegerán de acuerdo con su nivel de criticidad, mediante la implementación de controles de seguridad adecuados.
- **Inventario de activos de información:** Se realizará un inventario de activos de información, que incluirá la siguiente información:
    - Identificación del activo: Tipo de activo, nombre, número de serie, ubicación, etc.
    - Responsable del activo: Persona o área responsable del activo.
    - Clasificación del activo: Nivel de criticidad del activo.
    - Condiciones de seguridad del activo: Controles de seguridad implementados para proteger el activo.
- **Actualización del inventario:** El inventario de activos de información se actualizará de forma periódica, teniendo en cuenta cualquier cambio en la información o los activos.
- **Auditoría de activos de información:** Se realizará una auditoría de activos de información de forma periódica, con el fin de verificar la implementación y el cumplimiento de los controles de seguridad.

http://controlactivos.transitobucaramanga.gov.co:8880/login

este software se diseño con el fin de recolectar información de activos y esta data va servir para gestionarse en diferentes aspectos.

RESPONSABLE

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de retención y archivos de datos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

4. POLITICA DE PROYECTOS

RESUMEN. La presente política establece los lineamientos que se deben seguir en la ejecución de cualquier proyecto independiente de su naturaleza, asegurando la identificación y gestión de los riesgos en la seguridad de la información de estos.

INTRODUCCION. La seguridad de la información se debe concebir como parte primordial en la gestión de un proyecto, entendiendo el nivel de sensibilidad de la información, el riesgo asumido en cada una de las etapas de este y la aplicabilidad de controles establecidos en el desarrollo de cualquier proyecto.

ALCANCE. Aplica para todos los proyectos planeados y ejecutados por empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO. Establecer normas que identifiquen y gestionen los riesgos en la seguridad de información en el diseño y ejecución de proyectos en la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

Todo proyecto independiente de su naturaleza deberá asegurar que los riesgos de seguridad de la información se identifiquen y gestionen como parte de este; teniendo en cuenta como mínimo los siguientes requerimientos:

- Establecer los objetivos de seguridad de la información dentro del proyecto según los objetivos planteados.
- Incluir valoración de riesgos de seguridad en cada una de las etapas del proyecto, para identificar los controles necesarios.
- Garantizar en todas las fases de la metodología de proyectos, la aplicación de la seguridad de la información, además de los controles establecidos en la norma ISO 27001.

La gestión deberá ser permanente durante el ciclo de vida del proyecto y se deberán asignar los roles y responsabilidades de dicha labor dentro de la metodología de proyectos aplicada.

De igual manera se debe tener en cuenta el análisis y seguimiento de indicadores por proyecto y la identificación de lecciones aprendidas y mejores prácticas.

Requisitos de Seguridad

- Los controles de seguridad de la información deben ser proporcionales al nivel de riesgo, garantizando que sean efectivos y adecuados para la protección de los activos de información.
- La Oficina Asesora de Sistemas proporcionará capacitación periódica a los empleados y contratistas sobre la política de seguridad de la información y los proyectos tecnológicos.
- Todos los proyectos que involucren el uso, almacenamiento o procesamiento de información serán sometidos a una revisión de seguridad antes de su implementación para garantizar el cumplimiento de los controles y normativas de protección de datos.

RESPONSABILIDAD

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a los lineamientos de la política de proyectos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

5. POLÍTICA DE SEGURIDAD RELACIONADA AL ÁREA DE TALENTO HUMANO

RESUMEN. Esta política establece los lineamientos para procesos asociados a la selección y vinculación de personal a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA y tratamiento de datos personales.

INTRODUCCIÓN

El área de Recursos Humanos, desde su plan de capacitaciones, debe asegurar que los funcionarios y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA comprendan sus responsabilidades en relación con las políticas de seguridad de la información de la entidad y actúen de manera consistente frente a las mismas, para reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de esta.

ALCANCE. Esta política es aplicable a empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO.

Establecer lineamientos que permitan el correcto tratamiento de la información tanto de empleados y contratistas como la información propia de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIOS

- Fomentar el crecimiento personal y profesional de todas las personas que pertenecen al equipo de la entidad; haciéndoles partícipes del proyecto de éxito y socializando temas relevantes que contribuya al Personal.
- Establecer pautas que rijan las relaciones laborales en todas las áreas de la entidad y servir de referencia para definir los objetivos de la entidad en la gestión de los recursos humanos en cuanto a: la selección de sus profesionales, las garantías y estabilidad de un empleo de calidad, la creación de una relación estable con los trabajadores, la seguridad y salud laboral, así como la gestión y promoción del talento.
- La gestión de los recursos humanos debe salvaguardar y promover el respeto a la diversidad, la igualdad de oportunidades, la no discriminación y la alineación de los intereses de los profesionales con los objetivos estratégicos de la entidad.
- Realizar periódicamente evaluaciones del desempeño de El Personal de Planta de la enridad.
- Según el tipo de vinculación de personal a la entidad, el área de talento humano y/o la dirección deben reportar al líder de seguridad o comité de seguridad de la información el retiro de un empleado o contratista para revocar credenciales de acceso a los diferentes sistemas de información, verificar la entrega de la información y supervisar la correcta devolución de los equipos y recursos asignados al usuario de la red utilizando los formatos destinados para esto.
- De igual forma, el área de talento humano debe reportar los movimientos internos de personal de la entidad, y así ajustar los nuevos roles,
- Debe informar a Gestión Técnica y demás áreas autorizadas para generar accesos, sobre los retiros de personal, cambios y traslados, para que revoque los privilegios de acceso a los sistemas de información y datos sensibles del área a la que perteneció el empleado.
- Los contratistas y terceras partes deben acogerse a las políticas de seguridad física y las políticas de seguridad lógica implementadas en la entidad.
- Dar Capacitaciones al personal sobre la responsabilidad que tiene cada uno de los colaboradores.

RESPONSABILIDADES

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADO CLAVE

Dar cumplimiento a la política de seguridad en relación con el área de talento humano

6. POLITICA DE GESTION DE ACTIVOS DE INFORMACION

RESUMEN. Este documento define las políticas que se deben aplicar para la protección de los activos de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA a través de un proceso de clasificación de acuerdo con su nivel de importancia y sensibilidad.

INTRODUCCION.

Se considera información todo tipo de datos generados de manera digital, escrito en papel, formularios, o transmitido mediante una red de datos o dispositivos móviles de almacenamiento, lo cual constituye un estado de conocimiento.

Un activo de información es un elemento definido e identificado que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como valiosa para la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA; independiente del tipo de activo, es necesario considerar las siguientes características:

- Los activos no son fácilmente reemplazables y su alteración o daño representa costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Los activos forman parte de la entidad y su vulnerabilidad puede poner en riesgo las operaciones misionales y/o estratégicas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.
- La entidad registra y clasifica los activos de la información de acuerdo al estándar ISO/IEC 27001:2013.

ALCANCE.

Los Lineamientos de esta política deben ser aplicados a todos los funcionarios y contratistas que tengan uso directo de los activos de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO.

Establecer, clasificar y valorar los activos de información para que a través de los lineamientos que permitan la adecuada identificación y clasificación de los activos de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIOS.

- Se identifican los activos de información de mayor importancia asociados a cada Sistema de Procesamiento de la Información en su respectivo proceso, con sus responsables y su Ubicación, para luego elaborar un inventario con dicha información.

- El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información y los Activos asociados con los Medios de Procesamiento. Este debe ser revisado con una periodicidad no mayor a un (1) año.
- La responsabilidad de realizar y mantener actualizado el inventario de activos de información es de cada responsable de proceso de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.
- El uso de los activos de información pertenecientes a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información teniendo en cuenta el nivel de riesgo que ese activo tiene de acuerdo con su clasificación, y abstenerse de almacenar en ellos información no organizacional.
- Una vez se dé por terminada la relación con un empleado, cliente, contratista o tercero, se le deben retirar todos los privilegios de acceso a los recursos institucionales de la entidad y la persona deberá realizar la devolución de los activos que le hayan sido asignados o se encontrasen bajo su custodia durante su vinculación a la entidad.
- El responsable de cada proceso es el encargado de realizar la gestión para el retiro de acceso a los recursos institucionales que acarree la desvinculación de un cliente, empleado, contratista o tercero.
- Los colaboradores, contratistas, y en general los usuarios de la red, responsables de la información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, deben identificar los riesgos a los que está expuesta la información, teniendo en cuenta que esta pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo. Por lo tanto, se debe custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar su sustracción, destrucción, o uso indebido.
- Los procedimientos de seguridad de la información están bajo la responsabilidad de los líderes de área y estos deben asegurarse de que todos los miembros del grupo cumplan con las políticas y estándares de seguridad de la información de DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.
- Los líderes de las diferentes áreas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA son los responsables de mantener actualizado el inventario de los activos de información.
- El Personal de Planta, contratistas y terceros no podrán revelar a personas ajenas a la organización la información a la que tengan acceso en el ejercicio de sus funciones, de acuerdo con la guía de clasificación de la información y según sus niveles de seguridad.
- Las conexiones directas con los sistemas de cómputo y comunicaciones de otras entidades, a través de Internet o cualquier otro tipo de red, deben contar con una autorización previa.

RESPONSABILIDAD

Empleados, contratistas y terceros vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES.

- Establecer, clasificar y valorar todos los activos de la información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

7. POLITICA DE USO DE LOS ACTIVOS DE INFORMACION

RESUMEN. La presente política de uso de los activos de la información busca crear lineamientos que permitan la adecuada protección de los datos e información relevante para la Dirección de Tránsito de Bucaramanga por ello se debe concientizar a todos El Personal de Planta, contratistas y demás colaboradores sobre un manejo seguro y adecuado de los activos de información.

INTRODUCCION. La información es uno de los activos más valiosos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA debido a esto El Personal de Planta y contratistas que hacen uso de los activos que llevan esta información deben tener un alto nivel de compromiso siempre orientados al cumplimiento de la misión de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

Dirección de Tránsito de Bucaramanga es el propietario principal de los activos de información. Así mismo, los administradores de estos activos son El Personal de Planta y contratistas de la entidad y son ellos las personas autorizadas y responsables de la información generada en los procesos a su cargo, así como de los sistemas de información o aplicaciones informáticas, hardware o infraestructura tecnológica que tengan a su cargo.

ALCANCE. Esta política es aplicable a empleados, contratistas Y terceros que hagan uso de los activos de información pertenecientes a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO. Establecer normas que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de información que permitan la protección y el correcto uso de los activos de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIOS

- **Riesgo de seguridad de la información: Probabilidad de que un evento dañino ocurra y cause un impacto adverso en la confidencialidad, integridad o disponibilidad de la información.**
- **Clasificación de activos de información: Los activos de información se clasificarán de acuerdo con su nivel de criticidad, teniendo en cuenta los siguientes factores:**
    - **Importancia: Impacto de la información en el funcionamiento de la entidad.**
    - **Sensibilidad: Nivel de sensibilidad de la información, considerando su naturaleza y el impacto que su divulgación o modificación podría tener.**

- **Protección de activos de información: Los activos de información se protegerán de acuerdo con su nivel de criticidad, mediante la implementación de controles de seguridad adecuados.**

Inventario y Auditoría de Activos de Información

- **Inventario de activos de información: Se realizará un inventario de activos de información que incluirá:**
  - **Identificación del activo: Tipo de activo, nombre, número de serie, ubicación, etc.**
  - **Responsable del activo: Persona o área responsable del activo.**
  - **Clasificación del activo: Nivel de criticidad del activo.**
  - **Condiciones de seguridad del activo: Controles de seguridad implementados para proteger el activo.**
- **Actualización del inventario: El inventario de activos de información se actualizará de forma periódica, teniendo en cuenta cualquier cambio en la información o los activos.**
- **Auditoría de activos de información: Se realizará una auditoría de activos de información de forma periódica, con el fin de verificar la implementación y el cumplimiento de los controles de seguridad.**

Para más información y gestión de activos, acceda a: Sistema de Control de Activos

- No se pueden almacenar, instalar o utilizar software no autorizado en los equipos de cómputo de la entidad; de igual manera, no se podrán realizar cambios, ajustes o mejoras en la infraestructura física o lógica de aplicaciones instaladas en los equipos de cómputo.
- Todo el personal debe conocer y rendir cuenta por aplicar un mal uso de los activos de información. Estos actos incluyen él envió de correo electrónico masivo con fines no organizacionales, prácticas de juegos en línea, consultas a sitios web no permitidos, entre otros.
- Se hará seguimiento al correcto uso de los activos de la información.
- No se tolerarán situaciones que puedan poner en riesgo la organización y que no vayan de acuerdo con lo dicho en esta política.
- El responsable de TI revisará acuerdos en los niveles de Disponibilidad de servicio con los proveedores de Tecnología y proveedores de internet para asegurar los requisitos y necesidades de la entidad.

- El responsable de TI deberá Programar mínimo una vez al año pruebas de vulnerabilidades internas y externas para prevenir intentos de acceso a los recursos informáticos, prevenir la introducción y ataques cibernéticos.
- El líder de cada proceso gestionará ante el responsable de TI los cambios o modificaciones que se deban hacer sobre la infraestructura tecnológica.
- Los usuarios de los activos de información de la Dirección de Tránsito de Bucaramanga son los responsables de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Los usuarios de la red de datos deberán acceder a los sistemas de información utilizando una cuenta de usuario y una contraseña válida en la red.
- El responsable de cada proceso mantendrá un esquema de clasificación de los activos de información de la Dirección de Tránsito de Bucaramanga, de acuerdo con los niveles de seguridad establecidos en cada uno de los procesos, teniendo como base la información registrada en la gestión de activos de información, los cuales se encuentran en el formato de inventario de activos en el repositorio organizacional.
- El responsable de TI controla el software y los equipos autorizados que podrán ser utilizados por los usuarios de la red de datos de la entidad para la creación, edición y desarrollo de nuevos activos de información.
- El responsable de TI dispondrá de respaldos y será el encargado del restablecimiento de los programas que han sido adquiridos en los equipos asignados a cada uno de El Personal de Planta para el desempeño de sus actividades. El uso de programas sin su respectiva licencia y sin la autorización, obtenidos a partir de otras fuentes, puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que esta práctica no está autorizada.
- Ningún usuario de la red de datos de Dirección de Tránsito de Bucaramanga podrá copiar información clasificada o reservada sin la debida autorización.
- No se podrá utilizar la información de la entidad para otros fines; el usuario que infrinja esta norma será sancionado ya sea por copiar la información, sustraerla o causar algún daño sea intencional o no.
- Ningún equipo de cómputo presentará obsolescencia o daño irreparable, si esto pasa se tendrán los lineamientos correspondientes y necesarios para dar de baja el software y el equipo.
- Los activos de información pertenecen a la Dirección de Tránsito de Bucaramanga, y el uso de estos debe emplearse exclusivamente con propósitos laborales.

RESPONSABILIDAD
Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE
Dar cumplimiento a la política de uso de los activos de información

8. POLITICA DE ACCESO LOGICO

RESUMEN. Esta política establece los lineamientos para controlar el acceso a los activos de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, garantizando la debida protección de la información contenida en cualquier medio (digital/físico).

INTRODUCCION.

El control de acceso lógico es la primera línea de defensa para la mayoría de los sistemas, permitiendo prevenir el ingreso de personas no autorizadas a información propia de la entidad. Para controlar el acceso se emplean 2 procesos: identificación y autenticación.
La identificación se entiende como el momento en que el usuario se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esa identificación.

Para la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA es prioritario definir el personal que tenga acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de esta.
La plataforma tecnológica es responsabilidad de la Oficina de TI, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos.

La Secretaria General es responsable de garantizar entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en oficinas, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

ALCANCE Esta política aplica a toda la información contenida en cualquier medio (digital o físico), áreas de procesamiento de información, redes de datos, recursos de la plataforma tecnológica y sistemas de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, además para todo el personal empleado y contratista y terceros que tengan acceso a las instalaciones de la Entidad y sistemas de información.

OBJETIVO Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

PRINCIPIO

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud al área respectiva.

- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.

- Se deberá deshabilitar o borrar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

- Se deberán realizar revisiones periódicas en los diferentes sistemas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.

- Cada miembro del personal de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.

- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

    - El jefe de área o líder de proceso deberá ser el único autorizado para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario, a través de las diferentes categorías de la mesa de ayuda.

    - La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema) y de las áreas responsables de dicho activo.

    - El jefe de área o Líder de proceso deberá establecer los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y los sistemas de información.

    - Los administradores de cada aplicación (sistema) deberán crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por el jefe de área o líder de proceso.

    - Se deberá establecer un procedimiento de entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, a los recursos de la plataforma tecnológica o a los sistemas de información.

- Se deberán inhabilitar o eliminar los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica.

- Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

- Se deberá establecer controles de acceso a los ambientes de producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.

- Se deberán establecer mecanismos de auditoria al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.

- Se deberá identificar al personal que requiere acceso a las instalaciones de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.

- Se deberá contar con mecanismos de control de acceso para las áreas seguras (el centro de cómputo, la unidad de diagramación administración de infraestructura y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA considere pertinentes.

- Las puertas de acceso al centro de cómputo, unidad de diagramación, administración de infraestructura, y centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.

- Se deberá aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura, unidad de diagramación o a los centros de cableado, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.

- Se deberá registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado en una bitácora ubicada en la entrada de estos lugares de forma visible.

- Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

- Se deberá bloquear de manera inmediata los privilegios de acceso físico a las instalaciones de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA tan pronto el personal termine su vinculación.

- Se deberá realizar la devolución del carné institucional tan pronto el personal termine su vinculación con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

- Se deberá implementar controles de acceso físico al centro de cómputo para evitar la manipulación no autorizada del cableado.

RESPONSABILIDAD

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de acceso lógico de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

9. POLITICA DE ACCESO FISICO AL DATA CENTER

RESUMEN. La presente política establece las reglas para acceso físico al centro de datos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, teniendo en cuenta su acceso por empleados y/o contratistas autorizados, con videovigilancia, sistema de alarma y detección de incendios.

INTRODUCCION. La seguridad física de la data center de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA implica proteger la infraestructura critica de amenazas externas o intrusiones que atente contra las actividades de la entidad.
La seguridad física de los data centers implica proteger la infraestructura crítica de amenazas externas o intrusiones que atenten contra las actividades de una entidad. Elementos de alto valor y sumamente importantes, tales como servidores, switches y unidades de almacenamiento.
Este tipo de seguridad incluye videovigilancia a través de cámaras, sistemas de control de acceso y seguridad perimetral.

ALCANCE. Esta política va dirigida a empleados y contratistas que tengan acceso a la infraestructura de la data center de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO
Definir lineamientos que permitan un acceso seguro y adecuado a la infraestructura de la data center de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

Para un acceso seguro se debe tener un usuario y contraseña registrados en forma previa, es responsabilidad del usuario velar por la confidencialidad de la credencial de acceso.

Hay sistemas de vigilancia de vídeo y sensores de detección de movimiento en funcionamiento continuo. La actividad dentro de los centros de datos y fuera de la entidad es controlada y grabada en servidores seguros, al tiempo que hay un equipo de vigilancia en sitio 24/7.
Con el fin de controlar y supervisar el acceso a las instalaciones, se han implementado procedimientos estrictos de seguridad. Cada miembro del personal tiene una placa RFID (Tarjeta de identificación mediante radio frecuencia) nominal para restringir su acceso. Los derechos de acceso de El Personal de Planta son revisados regularmente. Para acceder a las instalaciones, El Personal de Planta deben presentar sus insignias para la verificación, antes de pasar por las puertas de seguridad.

El fuego es otro riesgo controlado. Cada sala del centro de datos está equipada con detectores de fuego y sistemas de extinción, así como puertas cortafuego. Los data centers cumplen con la norma APSAD R4 para la instalación de extinguidores, además cuenta con la certificación N4 de conformidad.

RESPONSABILIDAD

Empleados y contratistas vinculados con la Dirección de Tránsito de Bucaramanga

RESULTADO CLAVE

Dar cumplimiento a la política de acceso físico al data center de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

10. POLITICA DE CONTROL DE ACCESO A LAS REDES

RESUMEN La presente política establece los lineamientos que la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA debe tener para vigilar el acceso no autorizado a los servicios de red.

INTRODUCCION

Los equipos suelen formar parte de una **red** de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos, debido a esto la política de control de acceso de las redes logra impedir el acceso no autorizado a los servicios en la red.

ALCANCE Esta política va dirigida a empleados y contratistas que tengas acceso a la red de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO

Establecer una política que controle el acceso a la red de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

- Impedir el acceso no autorizado a los servicios de la red.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se ingrese a la red por medio de computación móvil e instalaciones de trabajo remoto.
- Se deberían controlar los accesos a servicios internos y externos conectados en red.

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

- Existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones.
- Que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos.

RESPONSABILIDAD

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de control de acceso a redes

11. POLITICA DE USO DE PUNTOS DE RED Y CONTROL DE ACCESO A LA LAN

RESUMEN. La presente política establece los parámetros necesarios para uso de puntos de red y el acceso adecuado a la red de área local de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, con el fin de preservar la disponibilidad, confidencialidad e integridad de la información.

INTRODUCCION El acceso a la red es el primer aspecto que se debe tener en cuenta una vez instalado el software de red, garantizando que cada empleado o contratista tenga acceso al servicio.
Una red de área local permite que los dispositivos se conecten, transmitan y reciban información entre ellos, utilizando herramientas de seguridad que permitan la protección de los mismos.

ALCANCE Esta política es aplicada a empleados y contratistas que hacen uso de puntos de red y tienen acceso a la red de área local de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO. Establecer lineamientos que permitan un correcto de la red de área local de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, así como el uso adecuado de los puntos de red.

PRINCIPIO

- Los usuarios deben usar las redes LAN de la entidad de manera ética, razonable, responsable, no abusiva y sin afectar la disponibilidad, confidencialidad o integridad de la información de la entidad.
- A la red LAN de la entidad solamente deben conectarse los computadores de la entidad y su uso debe ser exclusivamente para fines laborales.
- Los usuarios no deben conectar a la red LAN dispositivos de red no pertenecientes a la entidad, como routers, módems, switchs, repetidores o access points, entre otros.

RESPONSABILIDAD

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADO CLAVE

Dar cumplimiento a la política de control de uso de puntos de Red y control de acceso a la LAN

12. POLITICA DE GESTION DE CLAVES DE ACCESO A LOS SISTEMAS DE INFORMACION

RESUMEN. Esta política hace referencia a los parámetros que garantizan la adecuada vigilancia en la protección de los sistemas de información mediante control de acceso a la información almacenada en la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

INTRODUCCION. Dirección de Tránsito de Bucaramanga identifica la información como un componente indispensable para la entidad, por esta razón establece la política de gestión de claves de acceso a los sistemas de información, protegiendo adecuadamente la recolección de dicha información, a través de contraseñas con un nivel alto de seguridad que solo manejen usuarios con sus respectivos roles. Para la elaboración del mismo se toman en cuenta las

regulaciones aplicables según el sistema de seguridad de la entidad y la política de administración de contraseñas.

ALCANCE. Esta política aplica para todos los funcionarios, contratistas y terceros que tengan acceso a los sistemas de información de la entidad Dirección de Tránsito de Bucaramanga.

OBJETIVOS.

Establecer lineamientos que permitan la adecuada gestión de control de acceso a los sistemas de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, manteniendo la confidencialidad, integridad y disponibilidad de la información.

PRINCIPIOS.

- Sensibilizar a los usuarios en cuanto a la responsabilidad en el uso de las buenas prácticas de seguridad en la selección, uso y protección de las credenciales de acceso a los sistemas de información con el fin de preservar la integridad de la información.
- Garantizar el uso de herramientas seguras cuando se trabaje de forma remota.
- Todos los colaboradores deben tomar medidas de seguridad, terminando las sesiones activas cuando finalice su actividad o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
- Las contraseñas no deben ser reveladas a ninguna persona, y no deben ser registradas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y que el método de almacenamiento esté aprobado por el comité de seguridad.
- Las cuentas de usuario y contraseña de administradores son de uso personal e intransferible, con su respectivo respaldo bajo herramientas seguras en el director de área y gerencia.
- Los sistemas de información deben tener un protocolo para recuperar las contraseñas en dado caso que se presente algún siniestro.
- Se tendrá la trazabilidad de asignación y retiro de las credenciales de usuario que tengan acceso a información de la entidad.
- Se tomarán acciones cuando se afecte la información debido a la omisión de alguna de las políticas anteriores; de igual manera cuando por una mala gestión de contraseñas los resultados no sean los deseados.
- Los usuarios de la red de datos son los directamente responsables del uso de las claves o contraseñas de acceso que se le asignen, o ellos mismos establezcan para la utilización de los equipos y/o servicios informáticos de la Dirección de Tránsito de Bucaramanga.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar el procedimiento de resguardo y custodia de las claves o contraseñas en un sitio seguro, utilizando herramientas que permitan la protección de dichas claves. A esta herramienta solo debe tener acceso el responsable de asignación de contraseñas y la gerencia de la entidad.

- Empleados, contratistas y terceros deben emplear obligatoriamente contraseñas con un alto nivel de complejidad de acuerdo con el rol asignado y la importancia de la información que maneje.
- En toda la política se tendrá en cuenta las posibilidades de fraude asociado al abuso de los sistemas de información.

RESPONSABILIDADES

Empleados, contratista y terceros vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES

Dar cumplimiento a los lineamientos de la política de claves de acceso a los sistemas de información.

13. POLITICA DE ADMINISTRACION DE CONTRASEÑAS

RESUMEN. Esta política establece las pautas necesarias para la creación correcta y segura de una contraseña, la protección y el cambio cada cierto tiempo de esta, mejorando la seguridad en los sistemas de información buscando una mejor protección de los datos en la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

INTRODUCCIÓN

Las contraseñas son un aspecto muy importante de la Seguridad de la Información. Una contraseña débil puede dar lugar a accesos no autorizados y/o explotación de recursos de la entidad. Todos los usuarios, incluyendo contratistas y proveedores con acceso a sistemas de la entidad, son responsables de tomar las medidas adecuadas para seleccionar y proteger sus contraseñas.

ALCANCE

Esta política se aplica a todo el personal que tenga asignada una contraseña para el inicio de sesión de cualquier herramienta de software que maneje la organización Dirección de Tránsito de Bucaramanga.

OBJETIVO

Establecer un estándar de uso de contraseñas seguras, la protección de estas y su frecuencia de cambios.

PRINCIPIO

- Todo empleado que sea hallado como transgresor de esta política puede estar sujeto a medidas disciplinarias, que pueden incluir hasta terminación del contrato, dependiendo de la gravedad de la falta.
- No se debe permitir que individuos que no sean miembros de la entidad tengan acceso a los servicios de cómputo y comunicaciones de la Dirección de Tránsito de Bucaramanga. Todos El Personal de Planta, contratistas y terceros deben velar porque este tipo de situaciones no se presenten al interior de la entidad.
- Cada contraseña es de uso personal e intransferible. El Personal de Planta no deben revelar la contraseña de su cuenta a otros y/o terceros. Se debe notificar inmediatamente al responsable de TI o al comité de seguridad si sospechan que alguien ha obtenido acceso sin autorización a su cuenta y debe modificarla en forma inmediata. Cualquier excepción a la norma debe ser aprobada por el personal encargado de Dirección de Tránsito de Bucaramanga con antelación.
- Está prohibido enviar la contraseña por el correo electrónico, (teniendo en cuenta que este no es un medio seguro) o mencionarla en una conversación
- Para el buen uso de las contraseñas se debe tener en cuenta los siguientes aspectos:

    - Las contraseñas deben ser construidas con mínimo ocho (8) caracteres, deben incluir mayúsculas, minúsculas, números y caracteres especiales.
    - No utilizar contraseñas que sean únicamente palabras o nombres (aunque sean extranjeras).
    - No utilizar contraseñas completamente numéricas con algún significado (teléfono, fechas, direcciones, nombres, lugares).
    - Cambiar la contraseña 4 veces al año; cada 3 meses.

RESPONSABILIDADES

Empleados, contratista y terceros vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES

Dar cumplimiento a la política de administración de contraseñas.

14. POLITICA DE ESCRITORIO Y PANTALLA LIMPIA

RESUMEN. Esta política establece las normas a tener en cuenta por parte de empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, para el correcto manejo de documentos e información que se encuentren en los puestos de trabajo y equipos de cómputo durante y fuera del horario laboral evitando acceso no autorizado, perdida, daño y robo de información.

INTRODUCCION. Para tener un adecuado aseguramiento de la información que está bajo la responsabilidad de El Personal de Planta y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA se debe contar con una política de escritorio y pantalla limpios, adoptando buenas prácticas que permitan el correcto manejo de la información física y digital propia de la identidad que pueda ser alcanzada, copiada, no respalda o utilizada por terceros o por personal que no tenga autorización para uso o conocimiento.

ALCANCE. Esta política se aplica a todos los usuarios o trabajadores de la organización, dicha política sustenta la organización de la información, además, se aplica a todos los puestos de trabajo, instalaciones y equipos de cómputo y periféricos ubicados dentro de la entidad. Los usuarios de este documento son todos El Personal de Planta, contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO. Establecer lineamientos que permitan prevenir la perdida, daño, robo o compromiso de la información durante y fuera de las horas laborales en los puestos de trabajo y equipos de cómputo de El Personal de Planta y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIOS.

LA DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA sensibiliza a Todo el personal de planta y Contratistas para que adopten la política de escritorio y pantalla limpia realizando seguimiento de las directrices estipuladas para que se aborden siempre que sea necesario.

- Los sitios de trabajo de El Personal de Planta y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, deben localizarse en ubicaciones donde no queden expuestos al acceso de personas externas.
- Al ausentarse el empleado o contratista de su puesto de trabajo debe guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información pública de uso interno, clasificada o reservada al igual bloquear la sesión en su equipo de cómputo.
- Al finalizar la jornada laboral los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan cualquier tipo de información, estas deben guardarse en un lugar seguro y bajo llave.
- Los puestos de trabajo deben permanecer limpios y ordenados.
- Cuando se imprima o digitalice documentos estos deben retirarse de los equipos periféricos.
- Los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.
- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que empleados y contratistas cumplan con sus actividades diarias.

- Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.
- Si se utiliza un equipo portátil, debe mantenerse en un lugar seguro para evitar hurto del equipo.
- No dejar dispositivos extraíbles (USB, CD, DVD, Disco Duro Externo, etc) con información en lugares visibles o accesibles.
- Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarlo bajo llave
- Todo el personal debe conocer y rendir cuentas por la seguridad de la información en cuanto sea pertinente para su rol de trabajo.

RESPONSABILIDADES

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES
Dar cumplimiento a la política de escritorio y pantalla limpia.

15. POLITICA DE USO DE CORREO ELECTRONICO

RESUMEN. Esta política establece la responsabilidad y lineamientos mínimos que deben cumplir todos los usuarios de correo electrónico institucional asegurando el uso correcto del mismo como herramienta de trabajo de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

INTRODUCCION

Dirección de Tránsito de Bucaramanga ofrece a sus colaboradores el servicio de intercambio de mensajes a través de una cuenta de correo electrónico con dominio propio de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA utilizando la plataforma de ***Gmail***. Para facilitar el desarrollo de sus funciones, por lo tanto, los usuarios del correo electrónico son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Dirección de Tránsito de Bucaramanga se compromete a entregar un correo electrónico a sus empleados siguiendo lo estipulado en la política de correo electrónico, buscando de esta manera garantizar el uso adecuado de todos los sistemas contando con estrategias y medidas de seguridad de la información.

ALCANCE

Esta política aplica a los funcionarios, contratistas y terceros relacionados con Dirección de Tránsito de Bucaramanga que cuenten con una cuenta de correo corporativo de la entidad.

OBJETIVO

Establecer las responsabilidades y lineamientos mínimos que deben cumplir todos El Personal de Planta, contratistas y terceros que haga uso del correo institucional con el fin de garantizar la correcta función del mismo, asegurando un mejor aprovechamiento de esta herramienta de trabajo que provee la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIOS

El correo institucional es un medio formal y oficial de comunicación de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA siendo una herramienta de trabajo que facilita las funciones propias de El Personal de Planta y contratistas.

El desarrollo de esta política es con el fin de fomentar responsabilidad, respeto, integridad y seguridad de la información.

LA DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA se reserva el derecho de deshabilitar, modificar o eliminar la cuenta de correo electrónico institucional en las cuales se evidencie el uso inadecuado o incurran en el incumplimiento de las políticas plasmadas en este documento o el negocio lo requiera.

Para los usuarios pertenecientes a Dirección de Tránsito de Bucaramanga el servicio de correo electrónico se identificará de la siguiente manera: nombre de la cuenta según rol.área), seguido del: @dominio. El nombre para mostrar será equivalente al cargo o actividad a desempeñar; cualquier excepción al nombre debe ser aprobado con anterioridad por el personal encargado en la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

Los usuarios de los correos institucionales deben tener la responsabilidad de la clasificación de los correos spam.

- Emplear la opción de copia oculta (CCO) cuando se envía un mensaje de tipo informativo a más de una persona destinataria.
- Responder solamente al emisor del correo en caso de que se haya solicitado confirmación de recibido.
- Revisar las direcciones de los destinatarios antes de enviar el mensaje.
- Valorar la utilización de la opción de copia oculta para enviar un correo electrónico a múltiples destinatarios.
- Con objeto de no difundir injustificadamente direcciones de correo de terceros al reenviar un correo electrónico, valorar la opción de eliminar las direcciones de los destinatarios anteriores.
- Identificar de forma clara y concisa el asunto.
- No incluir datos personales en el asunto.
- Evitar palabras o expresiones que puedan activar los programas antispam.
- Revisar el contenido del mensaje, los archivos adjuntos y su destinatario antes de enviarlo.
- Emplear el pie de firma automático de los mensajes de correo electrónico, basados en el modelo establecido, que incluye la cláusula de confidencialidad. En caso de que el correo sea compartido identificar el nombre del emisor.

- Cuando se trate de mensajes con fines personales no se deberá utilizar el correo institucional.
- Evitar enviar archivos excesivamente grandes.
- Las claves de acceso a los correos electrónicos deben cumplir con la política de gestión de claves de acceso a los sistemas de información para asegurar un alto nivel de protección a la información.
- Los usuarios de correos institucionales de Dirección de Tránsito de Bucaramanga se hacen responsables de los procedimientos de copias de respaldo de su información, haciendo backup cada (dos) 2 meses.
- Los usuarios de los correos electrónicos se deben hacer responsables de la información que manejan y envíen mediante dicho correo, en caso de que el usuario borre de forma accidental algún correo o carpeta de su cuenta de correo corporativa de Dirección de Tránsito de Bucaramanga.

Los correos institucionales se emplearán única y exclusivamente para una finalidad operativa y administrativa y deben seguir los siguientes lineamientos:

- Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura tecnológica de la Dirección de Tránsito de Bucaramanga se consideran bajo el control de la entidad. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Dirección de Tránsito de Bucaramanga, y no debe utilizarse para ningún otro fin.
- Los usuarios del servicio de correo electrónico no deben realizar el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad o terceros.
- El servicio de correo electrónico no debe utilizarse para el envío de cadenas de mensajes.
- El servicio de correo electrónico de la Dirección de Tránsito de Bucaramanga no debe usarse para el envío de mensajes masivos y, en casos excepcionales, se debe utilizar la opción de copia oculta para todos los destinatarios.
- El servicio de correo electrónico de la entidad no debe ser utilizado para el envío de mensajes de gran tamaño que pueden congestionar la red; para ello deben emplearse otros medios como, por ejemplo, los servicios de la nube de archivos digitales ***(Google Drive, wetransfer)*** o en su defecto medios extraíbles como discos externos o memorias USB o mediante empresas de correspondencia certificada.
- A los usuarios del servicio de correo electrónico que se desvinculen de la entidad, se les bloqueara la cuenta de correo y esta misma será reemplazada en caso de que no haya cuentas disponibles o se necesite un nuevo correo electrónico, previa orden y autorización por parte de Gerencia o Talento Humano.
- A los usuarios de correos misionales o estratégicos en dado caso que se desvinculen de la entidad se bloqueara la cuenta de correo electrónico y se habilitara nuevamente hasta que sea reasignada al nuevo líder o encargado designado por gerencia.

- La apariencia de la firma de correo electrónico está establecida con los parámetros de la imagen de la entidad y ningún funcionario está autorizado para alterar la forma o la información contenida, teniendo en cuenta que la firma tendrá la siguiente información:
    - Nombre, cargo, empresa, número de contacto corporativo, direcciones físicas, página web, correo electrónico de contacto, logo de la entidad y política de confidencialidad de información.
- Garantizar que se mantengan los correos electrónicos procesados por todos los sistemas e infraestructuras tecnológicas que maneje la Dirección de Tránsito de Bucaramanga.

RESPONSABILIDADES

Empleados, contratistas y terceros vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADOS CLAVES

Dar cumplimiento a los lineamientos expuestos en la política de uso de correo electrónico.

16. POLITICA DE USO DE INTERNET
RESUMEN.

La política de uso de internet proporciona a El Personal de Planta las reglas líneas maestras acerca del uso apropiado de los equipos, la red y el acceso a internet de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, con el fin de proteger tanto a la entidad como al empleado y/o contratista.

INTRODUCCION

Internet es un recurso limitado y, por lo tanto, el uso debe ser para el interés de las actividades de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, toda información transmitida por este medio será tratada como información relacionada con la entidad.

ALCANCE

La presente política es aplicable a empleados, contratistas y terceros vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO

Establecer lineamientos que permitan tener un buen uso de internet para optimizar y facilitar funciones propias de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

- Establecer normas que aseguren el buen funcionamiento de Internet, para optimizar y facilitar sus labores de trabajo en DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.
- Establecer las normas que regulen el uso aceptable del servicio institucional de Internet por parte de El Personal de Planta y contratistas de la Institución, personal externo, terceros y/o pasantes autorizados, considerando al servicio de Internet como una herramienta de apoyo en la gestión y desempeño de sus funciones y actividades laborales.
- Proteger la Información almacenada en los computadores dentro de la infraestructura de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, evitando así las amenazas latentes por el uso indebido del servicio de Internet.
- La divulgación de información confidencial de la entidad en grupos de discusión, listas o chats está prohibida, independientemente si esta fue deliberada o involuntaria. Serán aplicadas las sanciones previstas en las políticas y procedimientos internos según lo dispuesto por la ley.
- El Personal de Planta con acceso a Internet solo pueden descargar programas directamente vinculados a las actividades de la compañía y deben proporcionar lo que sea necesario para regular la licencia y el registro de dichos programas.
- El Personal de Planta con acceso a Internet no podrán cargar ningún software con licencia o los datos que sean propiedad de la entidad sin el permiso expreso del gerente o responsable de TI.
- En esta organización no se permitirá el software de comunicación instantánea como Skype, WhatsApp y similares sin la debida autorización por parte del responsable de TI.
- Todo el personal debe conocer que no se permitirá el uso de software para descargar música, videos y otro contenido en formato Torrent.
- No se permitirá el uso de servicios de transmisión como Radios en línea o similares.
- El uso de las redes sociales se permitirá solo a los usuarios cuya actividad final, dependa de este tipo de acceso.
- Los usuarios de los servicios de internet de DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA deben hacer uso razonable de estos recursos y solo con propósitos laborales.
- No se permite la navegación a sitios con contenidos que representen peligro para la entidad como pornografía, terrorismo, *hacktivismo*, Deep web, segregación racial u otras fuentes asociadas a estos riesgos.
- Los usuarios de la red deben ser conscientes del uso adecuado de internet, y deben evitar el acceso a sitios potencialmente peligrosos o que puedan afectar el buen desempeño de la red.
- El responsable de TI inhabilitará el acceso a sitios web identificados como peligrosos, de alto consumo de recursos de red, o que afecten el desempeño del personal, a fin de proteger y no comprometer la seguridad y el desempeño de la red y los recursos informáticos de la entidad.
- La descarga de archivos de internet debe hacerse con propósitos laborales y de forma razonable para no afectar el servicio de Internet y la red de datos en general.
- No se permite la descarga por Internet de archivos de video, música, etc., por afectar el rendimiento de la red y uso del enlace de Internet.

- Cumplir las normas de uso aceptable del servicio institucional de Internet definidas en la presente Política.
- Cumplir con los procedimientos de autorización de servicios y recursos tecnológicos establecidos para tal efecto.
- Utilizar el servicio institucional de Internet, para asuntos relacionados con el desempeño de las funciones laborales o contractuales asociadas a la entidad DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.
- Los usuarios de servicios de internet de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA deben hacer uso razonable de los elementos y servicios suministrados por la entidad, además de utilizarlos sólo para propósitos laborales.
- No se podrá utilizar los recursos de la Compañía para descargar o distribuir software o datos no legalizados.
- Habrá bloqueo de acceso para archivos o dominios que comprometan el uso del ancho de banda o que interrumpan el buen funcionamiento de las labores de la entidad.

RESPONSABILIDAD
Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE
Dar cumplimiento a la política de uso de internet.

17. POLITICA DE TRANSFERENCIA DE INFORMACION

RESUMEN. Esta política establece las directrices para proteger el intercambio de información entre empleados, contratistas y terceros que estén vinculados con la Dirección de Tránsito de Bucaramanga por cualquier medio, teniendo como prioridad la integridad, disponibilidad y confidencialidad de la información propia de la entidad.

INTRODUCCION

Para el cumplimiento de sus obligaciones la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA intercambia información entre empleados, contratistas, terceros y diferentes entes y por diferentes medios, por ello es necesario establecer unos lineamientos que garanticen que el intercambio de dicha información se realiza bajo los niveles de protección adecuados siempre que se vaya a transferir información personal, información pública clasificada o pública reservada, quien está enviando la información deberá: confirmar que cuenta con la autorización expresa del titular del dato o su representante para su tratamiento.

ALCANCE

Esta política aplica a toda la información contenida en los sistemas de información, bases de datos, archivos físicos o electrónicos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, alojados en cualquier medio electrónico (servidores, estaciones de trabajo, medios de almacenamiento removibles, etc.) o físico (Carpetas, libros, formatos, etc.), que requiera ser entregada.

Esta política aplica a todos las, personas, instituciones y colaboradores, ya sean funcionarios de planta, contratistas, estudiantes en práctica y terceros (proveedores, compra de servicios, etc.), que participen en la transferencia de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO

Establecer lineamientos que permitan mantener la seguridad de la información en el intercambio de la misma entre empleados, contratistas y terceros de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

Solo se puede realizar intercambio de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA entre su personal cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus labores.

Siempre que se realice intercambio de información catalogada como pública clasificada o pública reservada, dicho intercambio debe ser aprobado por el jefe directo o supervisor de contrato.

Todo intercambio de información electrónica perteneciente a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA con terceros, debe ser respaldado con un acuerdo (convenio o contrato), incluyendo una cláusula de confidencialidad y no divulgación de la información proporcionada.

La solicitud de intercambio de información puede ser por requerimientos de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, del organismo externo o incluso de un tercero que, ante disposiciones legales o directrices del gobierno hacen necesaria dicha interoperabilidad.

La excepción en la entrega de información debe estar regida por lo establecido según legislación vigente.

La información recibida de otra entidad en Colombia se debe salvaguardar a un nivel igual o mayor que el aplicado por la entidad que originó el documento.

El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.

El intercambio de información que se encuentre en formatos físicos debe estar debidamente etiquetada, en caso de que sea catalogada como pública clasificada o pública reservada, el intercambio debe realizarse en un sobre sellado para ser enviada a terceros.

Para el transporte de medios físicos de información sensibles, se debe generar una bitácora de entrega de estos medios y recepción de estos.

Se debe transportar en un dispositivo con un sello de seguridad que garantice que en su desplazamiento no ha sido intervenido por un tercero.

Para la apertura de ese sello se debe generar un registro y garantizar que no se reutilice el sello.

Se deben transportar estos medios en un recipiente que proteja al activo de amenazas ambientales.

Toda información enviada desde la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA a través de correos electrónicos deberá incluir en su pie de página la siguiente advertencia:

Este mensaje y cualquier archivo que se adjunte al mismo es confidencial y podría contener información clasificada y reservada de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borrar el mensaje recibido inmediatamente.

RESPONSABILIDAD

Empleados, contratistas y terceros vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de transferencia de información estipulada por la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

18. POLITICA DE USO DE DISPOSITIVOS DE ALMACENAMIENTO

RESUMEN. Esta política establece los lineamientos para el correcto uso de dispositivos de almacenamiento extraíbles (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc), los cuales permiten una transferencia rápida y directa de la información. Se debe aplicar las medidas de seguridad que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus

Si se necesita almacenar información sensible o confidencial se utilizarán dispositivos externos corporativos debidamente protegidos, se almacenarán en lugares seguros y se informará al responsable si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.).

INTRODUCCION

Los medios de almacenamiento extraíbles permiten transportar y respaldar información de manera más fácil. Para asegurar la información contenida en los dispositivos extraíbles se deben aplicar medidas de seguridad como: cifrar los datos almacenados, establecer permisos de acceso, cambiar periódicamente la contraseña, etc. Otro de los aspectos importantes a

tener en cuenta es la eliminación de la información almacenada. Para asegurar que estos datos no volverán a ser accesibles, debemos utilizar los métodos de borrado seguro: destrucción física del dispositivo, desmagnetización o sobreescritura según convenga en cada caso. En definitiva, debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren, así como concientizar a El Personal de Planta y contratistas para su buen uso. De esta forma protegeremos tanto la información contenida en ellos como la de los dispositivos a los que se conectan.

. Esta política se aplica a quienes hagan uso de equipos móviles y dispositivos de almacenamiento removible de propiedad de la entidad y de propiedad de terceros cuyo uso haya sido autorizado.

OBJETIVO Establecer normas de uso de los dispositivos extraíbles que garanticen la seguridad de la información institucional **ALCANCE** que almacenan y la de los equipos a los que se conectan.

PRINCIPIO

El responsable del dispositivo de almacenamiento extraíble deberá velar por el buen uso de la información restringida almacenada en el mismo, su adecuado control y distribución limitada. También deberá usar mecanismos de protección como el uso de contraseñas y/o encriptación de archivos.

El responsable del dispositivo de almacenamiento extraíble, deberá adoptar las medidas que se encuentren a su alcance para asegurar que los archivos contenidos en él se encuentren libres de virus, software y/o código malicioso que pueda poner en riesgo la confidencialidad, integridad y disponibilidad de la información y los equipos informáticos de la entidad.

RESPONSABILIDAD

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADO CLAVE

Dar cumplimiento a la política de uso de dispositivos de almacenamiento.

19. POLITICA DE USO DE REDES SOCIALES CORPORATIVAS

RESUMEN. Las redes sociales han modificado la forma de comunicarnos e interactuar; es de gran beneficio utilizar medios sociales digitales para intercambio de información con criterio adecuado y sentido común. Esta política establece los lineamientos para el correcto uso de las redes sociales corporativas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

INTRODUCCION.

Una política de redes sociales describe la forma en que una organización y sus empleados deben comportarse en los medios digitales. El presente documento ayuda a proteger la reputación de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, al tiempo que motiva a El Personal de Planta y contratistas a compartir el mensaje de la entidad con responsabilidad. Puesto que las redes sociales evolucionan con rapidez, esta política debe considerarse como un documento abierto; serán necesarias las actualizaciones constantes.

ALCANCE

Esta política está dirigida a empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que tengan acceso y hagan uso de las redes sociales corporativas.

OBJETIVO Establecer lineamientos que permitan el manejo adecuado y con sentido común en las publicaciones a título personal o de la entidad y que no comprometan a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA en situaciones problemáticas e innecesarias.

PRINCIPIO

El Personal de Planta y contratistas no deben asumir en nombre de la entidad, posiciones personales en redes sociales u otros medios similares que se encuentren en internet.

Las redes sociales institucionales deben ser usadas exclusivamente por el personal autorizado y para fines exclusivamente institucionales.

Los usuarios deben usar los sistemas de mensajería instantánea provistos por la entidad de manera ética, razonable, responsable, no abusiva y sin afectar la disponibilidad, confidencialidad o integridad de la información de la entidad.

Los usuarios deben usar el servicio de mensajería instantánea provisto por la entidad exclusivamente para asuntos laborales.

RESPONSABILIDADES

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADOS CLAVES

Dar cumplimientos a la política de uso de redes sociales corporativas.

20. POLITICA DE RESPALDO Y RESTAURACION DE LA INFORMACION

RESUMEN. El presente documento establece los lineamientos aplicables a los sistemas de información y a la infraestructura de servidores de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA en lo referente al respaldo y restauración de información.

INTRODUCCION

Cualquier dispositivo de almacenamiento masivo tiene la posibilidad de fallar por esto, La DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA ha determinado la necesidad de contar con una política de respaldo y restauración de información garantizando la disponibilidad e integridad de la información al administrador y líder de servicio de tecnología para reducir el impacto de los riesgos generados en fallas de prestación de servicio que involucren la pérdida total o parcial de la información.

ALCANCE.

Esta política aplica a Todo el personal de planta y Contratistas que sean responsables de administrar, liderar, gestionar e interactuar con la infraestructura tecnológica, sistemas de información y dispositivos de almacenamiento masivo que contengan información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA para la prestación del servicio.

OBJETIVO

Definir lineamientos que permitan tener un correcto respaldo y restauración de información con el fin de preservar la integridad, confidencialidad y disponibilidad de la información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

PRINCIPIO

- DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA adoptará planes de recuperación de emergencia para todas las aplicaciones que manejen información crítica, y sean responsabilidad de la entidad. Dichas copias se actualizarán periódicamente, y se verificara el respaldo correcto.
- DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA mantendrá al menos una copia de la información en un servidor de archivos ubicado en el (Data center) de la entidad, esto para las aplicaciones de tipo local. para aquellas que están en la nube, se realizará un proceso de copias de respaldo.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información. A su vez, se realizarán periódicamente pruebas de funcionamiento y ejecución de los procesos de *backup*.
- Las copias de seguridad del servidor de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA se harán de forma automática y se deben sacar con discos duros extraíbles que siempre permanecerán en el sitio y se eliminará la información semanalmente con el fin de generar espacio de almacenamiento efectuando un proceso de borrado seguro y posteriormente la eliminación o destrucción en forma adecuada.

- Los respaldos de información sensible, crítica y valiosa deben almacenarse en un sitio protegido contra inclemencias del medio ambiente y con controles estrictos de acceso que se encuentre a una distancia razonablemente fuera del alcance de un evento en la zona original.
- Si se otorga a los usuarios finales la capacidad de restaurar sus archivos propios, no deben tener los privilegios para restaurar los archivos de otros usuarios o examinar qué archivos han sido respaldados por otros usuarios.
- Todos los colaboradores de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA conocerán la información confidencial según su rol de trabajo.
- Se harán reportes de la información a la que se les realizo backups.
- No serán tolerables pérdidas de información por la inexistencia del backup de la misma.
- Todas las copias de información crítica de DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA deben almacenarse en un área adecuada y con un control de acceso. Estas copias se mantendrán con el propósito de tener un respaldo y restauración de los sistemas en caso de la materialización de una amenaza, como pueden ser: defecto en los discos de almacenamiento, problemas en los servidores y computadores, virus o ataques informáticos, catástrofes naturales o provocadas por el hombre.
- Los administradores de los servidores de backups (tercerizado) realizarán periódicamente pruebas de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas controlado.
- Los usuarios deberán estar conscientes de que la información confidencial o sensible almacenada en sus computadoras puede ser recuperada con métodos avanzados aun cuando haya sido “normalmente” borrada. Por esta razón se deberán tener las precauciones para el manejo de información Confidencial en las computadoras y memorias USB, que hayan tenido esta información y que se pretendan prestar o compartir.

RESPONSABILIDAD

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADOS CLAVES

Dar cumplimiento a la política de respaldo y restauración de información.

21. POLITICA DE PROTECCION CONTRA CODIGO MALICIOSO

RESUMEN. El presente documento establece los lineamientos necesarios para la protección adecuada contra código malicioso; detectando, previendo y recuperando información contra un código no autorizado.

INTRODUCCION. El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los

peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, introducir controles para evitar, detectar y retirar los códigos maliciosos.

ALCANCE. El alcance de los lineamientos que se definen en esta política da cubrimiento a los accesos que involucren:

- Hardware (servidores, equipos de cómputo portátiles y de escritorio, medios de almacenamiento externo, como memorias externas USB, CD (Discos Compactos) y DVD.
- Software no autorizado por el área de TI.
- Acceso a internet.
- Red Interna (Intranet)

Aplica para todos los Servidores Públicos de la Entidad: Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas y demás personal que tenga acceso a los equipos de cómputo y a la red de la entidad.

OBJETIVO

Establecer lineamientos que permiten un control adecuado contra código malicioso.

PRINCIPIO.

Definir las medidas de prevención, detección y corrección frente a amenazas causadas por códigos maliciosos en Dirección de Tránsito de Bucaramanga.

- Está prohibida la descarga y/o instalación de software no autorizado. Si se necesita instalar programas que no se encuentren en la lista autorizada se deberá contar con autorización del administrador de TI. La lista de software autorizado se encuentra dentro de cada documento de los diferentes cargos de Dirección de Tránsito de Bucaramanga.
- Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.
- La red de servidores y computadores de Dirección de Tránsito de Bucaramanga deberá tener instalada una plataforma de hardware y software de ANTIVIRUS para evitar la propagación de software malicioso.
- La plataforma de ANTIVIRUS debe cumplir los siguientes requerimientos:
    - Consola centralizada de administración.
    - Actualización de la base de datos de virus o amenazas para los antivirus de forma permanente, automática y centralizada.
    - Distribución de actualizaciones automática de las estaciones de trabajo.
    - Monitoreo centralizado.
    - Debe verificar la presencia de código malicioso en todos los archivos en ordenadores, dispositivos magnéticos y servidores.
    - Debe verificar la presencia de código malicioso en los adjuntos y las descargas del correo electrónico antes del uso, esta verificación se debe efectuar en los

servidores de correo electrónico, los ordenadores y cuando ingresan a la red de Dirección de Tránsito de Bucaramanga.
    - Debe verificar las páginas web para comprobar la presencia de código malicioso.
    - Configurar un alto grado de detección.
    - Bajo impacto en los tiempos de respuesta de las estaciones.
    - Proteger la totalidad de los computadores, servidores y equipos de la red para Dirección de Tránsito de Bucaramanga
    - Capacidad del Antivirus para ejecutarse en los diferentes sistemas operativos de Dirección de Tránsito de Bucaramanga.
- Todos los colaboradores y terceros que hacen usos de los servicios prestados por Dirección de Tránsito de Bucaramanga son responsables de manejo de antivirus para analizar, verificar y (si es posible) eliminarlos de la red, computadores, dispositivos de almacenamiento fijos, removibles, archivos, correos electrónicos que estén utilizando para el desempeño de sus funciones laborales.
- La instalación y manipulación del antivirus sólo puede realizarse por el responsable de TI
- Todos los equipos conectados a la red Dirección de Tránsito de Bucaramanga pueden ser monitoreados y supervisados por la oficina de TI.
- Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.
- Se deben llevar a cabo revisiones (mensuales, semestrales) del software y del contenido de datos de los sistemas. Se debe investigar la presencia de archivos no aprobados o modificaciones no autorizadas.
- El responsable de TI deberá recolectar y estar actualizado con información de diferentes tipos de malware y de cómo minimizar la probabilidad de infección. (Capacitarse periódicamente)
- Se deben hacer campañas de sensibilización a todos los trabajadores, colaboradores, terceros y clientes de ser el caso que no cuenten con políticas propias de control de código malicioso, con el fin de generar una cultura de seguridad de la información y minimizar los riesgos. Estas campañas están compuestas por:
    - Capacitaciones de concientización al ingreso de nuevo personal, y de manera anual al personal vigente.
    - Sensibilización de los diferentes tipos de malware y cómo prevenir una infección.
- Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por Dirección de Tránsito de Bucaramanga, cuyo origen sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.
- Los sistemas de cómputo que se sospechen han sido comprometidos por virus o software malicioso deben ser apagados y desconectados de la red en forma inmediata. El usuario debe solicitar apoyo técnico e informar al líder de área o al comité de seguridad.

- Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.
- Antes de restaurar archivos desde copias de respaldo, dichas copias deben ser evaluadas con el software antivirus de la entidad.
- Definir una política que dé cumplimiento a las licencias de software y que prohíba la instalación de software malicioso no autorizado.
- Establecer un control de acceso a la información.
- Concienciación y formación del personal.
- Realizar revisiones periódicas.
- Instalar y actualizar un sistema de antivirus e instaurar una política para utilizarlo con los ficheros adjuntos en un correo electrónico o con los que descargamos.
- Crear procedimientos para usar el antivirus, dar formación para su uso y para afrontar ataques.
- Disponer de un software espía, que se encargue de rastrear el trabajo que se realiza, y envíe dicha información a alguien externo.

RESPONSABILIDAD

Empleados y contratistas vinculados a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de protección contra código malicioso.

22. POLITICA DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

RESUMEN. Esta política establece normas para un adecuado análisis de requerimientos y controles para el desarrollo y mantenimiento de sistemas de información que brindan soporte a los procesos de la organización.

INTRODUCCION El desarrollo y mantenimiento de sistemas de información conlleva una serie de etapas que definen el flujo de actividades que se ejecuten con buenas prácticas para beneficio de la información propia de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

ALCANCE Esta política va dirigida a empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que tengan la responsabilidad del desarrollo y mantenimiento de los sistemas de información de la entidad.

OBJETIVO Establecer lineamientos que permitan el fortalecimiento y correcto y mantenimiento de los sistemas de información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA y cualquier software que contenga información.

PRINCIPIO

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos de la organización.
- El responsable de la seguridad de la información debe identificas y sugerir los controles a ser implementados en los sistemas desarrollados internamente o por terceros
- Verificar el cumplimiento de los controles establecidos para el desarrollo y Mantenimiento de sistemas.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas.
- El líder del área TI es el responsable de la administración de las técnicas criptográficas y claves; licenciamientos, calidad del software y la seguridad de la información en los contratos con terceros para desarrollo de software.

RESPONSABILIDAD

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADO CLAVE

Dar cumplimiento a la política de desarrollo y mantenimiento de sistemas de información

23. POLITICA DE DESARROLLO SEGURO

RESUMEN

Esta política establece un conjunto de reglas y practicas orientadas a proteger el uso inapropiado de la información por parte de El Personal de Planta y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA. Siendo la Oficina TIC la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollos, actualizaciones

e instalaciones de software. Además, de planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

INTRODUCCION

El desarrollo seguro permite generar un servicio, software y sistema seguro teniendo presente el resguardo de la información; para que esta protección sea de forma correcta la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA define una política que permite garantizar la seguridad de la información con buenas prácticas para cumplir de forma adecuada con el ciclo de vida de los sistemas de información.

ALCANCE Esta política está dirigida a empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA que hagan parte en sus funciones de actualizaciones e instalaciones de software.

OBJETIVO

Establecer una política que vigile y permita el cumplimiento de las buenas prácticas para el desarrollo seguro, además de establecer los criterios de seguridad considerados en las actualizaciones e instalaciones de software.

PRINCIPIO

Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software.

Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto

Se deberá establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.

Se deberá establecer un plan de actualización para el software que es desarrollado o se utiliza en la Entidad, asegurando que las últimas versiones y parches sean instalados lo antes posible, con el fin de evitar que alguna vulnerabilidad sea explotada.

El diccionario de datos, o repositorio de metadatos, deberá mantener una descripción actualizada de las definiciones de datos.

En el análisis de factibilidad de los requerimientos, se deberá considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.

Los requerimientos de seguridad deberán ser compatibles con lo que se establece en las demás políticas de seguridad de la información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

El nivel de confidencialidad de todos los elementos que componga el software deberá ser definido teniendo en cuenta la criticidad de los datos.

Si se utiliza un sistema gestor de bases de datos, se deberá emplear las herramientas de seguridad necesarias para garantizar el nivel de protección adecuado.

Todos los programas críticos deberán incluir la generación de registros de auditoría, considerando como mínimo la identidad del usuario que lee borra, escribe, o actualiza, el tipo de evento y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.

En la etapa de diseño se deberá proyectar el rendimiento esperado, con el objetivo de no sobre dimensionar los recursos necesarios para el funcionamiento del sistema (ancho de banda, RAM, recursos del servidor, etc.).

No está permitido modificar programas sin que quede registrado o documentado el cambio. En caso de requerirse la implementación de un cambio, este deberá ceñirse a los lineamientos descritos por la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

No está permitido escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.

En lo posible, las pruebas del sistema deberán incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.

En lo posible, las pruebas deberán ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, para permitir la verificación rápida y repetitiva.

Se deberán tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:

- Realizar las validaciones de datos de entrada y salida en un sistema confiable (por ejemplo: un servidor).
- Construir los aplicativos para que validen los datos de entrada y generen los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud, entre otros.
- Validar las entradas de datos con una lista “blanca” que contenga un directorio de caracteres aceptados.
- Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
- Limpiar las salidas de datos no confiables hacia consultas SQL, XML y LDAP o hacia comandos del sistema operativo.

Se deberán establecer los siguientes controles para la autenticación en los sistemas de información:

- Realizar los controles de autenticación en un sistema confiable (por ejemplo, un servidor).
- Si la aplicación administra un almacenamiento de credenciales, asegurar que únicamente se almacena el hash de las contraseñas.
- Validar los datos de autenticación, luego de haber completado todos los datos de entrada.

Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos:

- Realizar la creación de identificadores de sesión en un sistema en cual se confíe (por ejemplo: el servidor).
- Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la conexión asociada.
- No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.
- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Asegurar que la sesión expire después de cierto tiempo.
- No permitir la apertura de sesiones simultaneas con el mismo usuario.

Se deberá asegurar el manejo de operaciones sensibles en los aplicativos desarrollados, permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables (por ejemplo: el servidor).

Se deben considerar los siguientes aspectos en el manejo de errores:

- Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios. Los mensajes de error deben ser genéricos.
- Liberar espacio en memoria cuando ocurra una condición de error.

Para el manejo de archivos se deberán acatar las siguientes consideraciones:

- Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Prevenir la revelación de la estructura de directorios de los sistemas construidos.

Para el establecimiento de conexión a las bases de datos se deberán considerar los siguientes aspectos:

- No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas.

Se deberá remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

Se deberán desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y garantizar que dichos archivos solo tengan privilegios de lectura.

No se deberá incluir en parámetros, nombres de directorios o rutas de archivos. En su lugar, se deben utilizar índices que internamente se asocien a directorios o rutas pre-definidas.

Se deberá liberar la memoria previa a la salida de una función y de todos los puntos de finalización de la aplicación.

Se deberá garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

No se deberá permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Se deberán utilizar funciones de control de integridad (hash) para verificar la integridad del código interpretado, bibliotecas, ejecutables y archivos de configuración previo a su utilización.

Se deberá velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.

Se deberá efectuar sintonía o ajuste (tuning) de los controles establecidos en la fase de diseño.

Las aplicaciones deberán contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse la validación de captcha.

Las aplicaciones deberán contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.

Se deberá revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.

Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones más recientes puestas en producción, en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

RESPONSABILIDAD

Empleados y contratistas vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

RESULTADO CLAVE

Dar cumplimiento a la política de desarrollo seguro implementado por la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA

24. POLITICA DE REPORTE DE INCIDENTES DE SISTEMAS DE INFORMACION

RESUMEN. Esta política establece los lineamientos para poner en marcha unos reportes de incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para el manejo de los posibles incidentes de seguridad de la información que puedan presentarse al interior de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

INTRODUCCION. Se entiende como incidente de seguridad, cualquier evento que ponga en riesgo la integridad, disponibilidad y confidencialidad de la información de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA; Esta política contiene los componentes generales de la gestión de incidentes de seguridad y sus principales acciones, las cuales son aplicables en toda la organización y en toda información o activo de información sobre el cual se presente o exista un indicio de incidente de seguridad, generando confianza y responsabilidad en reportes de incidentes de seguridad de la información que se presenten en la entidad.

ALCANCE. Esta política es aplicable a todos El Personal de Planta, contratistas y terceros que detecten un evento o incidente de seguridad de la información, el cual deben reportar adecuadamente según los lineamientos establecidos por la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

OBJETIVO

Establecer normas que permitan dar gestión a los incidentes de riesgo de seguridad de la información advirtiendo y mitigando el impacto de estos.

PRINCIPIOS

- Dar a conocer los lineamientos generales definidos por Seguridad de la Información, para el manejo de los posibles incidentes de seguridad de la información que puedan presentarse al interior de la entidad.

- Generar un compromiso con El Personal de Planta de realizar el reporte al momento de ocurrir cualquier incidente de seguridad de la información al interior o con las aplicaciones propias de la entidad
- Establecer la afectación del activo de información, incluyendo el valor económico y la cantidad de información relevante para la entidad contenida en el mismo.
- Todo el personal de DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA debe estar vigilante respecto a los incidentes o debilidades de seguridad (incluyendo fallas en el sistema, pérdida del servicio, errores resultados de datos incompletos o inadecuados, rompimiento de la confidencialidad). Si se detectan estos incidentes o debilidades de seguridad, deben ser reportados en forma inmediata al encargado de seguridad al email: XXXXXXXXXXX
- El personal encargado debe proceder de acuerdo con las instrucciones de la brigada de emergencias y según lineamientos de los cuerpos de socorro, privilegiando la conservación de la vida e integridad de las personas tanto de la Superintendencia Nacional de Salud como de visitantes.
- Los usuarios son la primera línea con la que se pueden identificar eventos adversos sobre la información o algún activo de información, y es de su responsabilidad y deber reportar cualquier situación anormal que pueda llegar a convertirse en un incidente de seguridad de la información.
- Un colaborador, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad, debe notificarlo a la mesa de ayuda quién será el primer punto de contacto.
- El encargado de la seguridad de la información es el responsable de coordinar los esfuerzos necesarios para dar atención a un incidente dentro de la entidad, de igual manera, tiene la responsabilidad de informar a los respectivos niveles administrativos de los incidentes y su grado de severidad dentro de la entidad, así como coordinar los esfuerzos con empresas externas en caso de ser necesario.

RESPONSABILIDAD

Empleados y contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de reporte de incidentes de los sistemas de información.

25 POLITICA DE CUMPLIMIENTO ANTE REQUERIMIENTOS LEGALES Y CONTRACTUALES

RESUMEN La presente política estable los lineamientos que garantizan que la seguridad de la información es implementada y operada de la manera adecuada permitiendo una correcta revisión y mejora continúa evitando incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad, que pueda tener como consecuencia para la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA algún tipo de multa o demanda.

INTRODUCCION Es política de Dirección de Tránsito de Bucaramanga, el cumplimiento de todas las obligaciones legales, adquiriendo el material patentado de la entidad propietaria. Todo el software web y móvil prestado a nuestros clientes son propiedad de Dirección de Tránsito de Bucaramanga y siempre se deben registrar en la superintendencia de industria y comercio (Dirección nacional de derecho de autor) como lo es el logo, la mascota, las aplicaciones web y móvil, entre otro dado el caso.

ALCANCE. Esta política se aplica a Todo el personal de planta y Contratistas de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA, sustenta la organización de la información, además, se aplica a todos los puestos de trabajo, instalaciones y equipos ubicados dentro de la entidad.

OBJETIVO.

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información, asegurando que se revisen y actualicen periódicamente.

PRINCIPIO.

Identificar y documentar explícitamente todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA para cumplirlos y mantenerlos actualizados para cada sistema de información y para la organización.

Documentar los controles y las responsabilidades individuales para cumplir estos requisitos estatutarios, reglamentarios y contractuales.

Identificar toda la legislación aplicable a la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA para cumplir los requisitos emitidos por entes reguladores.

Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intel ectual y el uso de productos de software patentados.

Asegurar la protección de cualquier material que se pueda considerar propiedad intelectual, teniendo en cuenta los siguientes lineamientos: o

- Publicar una política de cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos.
- Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violen los derechos de autor.
- Mantener conciencia de las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias contra el personal que las incumpla.

- Mantener los registros de activos apropiados, e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual.
- Mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc. o Implementar controles para asegurar que no se exceda el número máximo de usuarios permitido dentro de cada licencia.
- Llevar a cabo revisiones para verificar que solo hay instalados software autorizado y productos con licencia. o Definir una política para mantener las condiciones de licencia apropiadas. o Definir una política para disposición o transferencia de software a terceros.
- Cumplir con los términos y condiciones para el software y la información obtenida de las redes públicas.
- Duplicar, convertir a otro formato o extraer de registros comerciales solo lo que permita la ley de derechos de autor.
- No copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor

Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

Proteger los registros (por ejemplo, registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales) contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

Clasificar los registros por tipos, por ejemplo, registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, cada uno con detalles de los períodos de retención y tipo de medio de almacenamiento permisible, por ejemplo, papel, microfichas, medios magnéticos, medios ópticos, almacenamiento en nube. Cualquier llave criptográfica y programas relacionados asociados con archivos permanentes encriptados o firmas digitales, también se deben almacenar de manera segura para posibilitar la desencriptación de los registros durante el tiempo en que están retenidos.

Para salvaguarda los registros, se deberían realizar los siguientes pasos dentro de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA:

- Emitir directrices acerca de la retención, almacenamiento, manejo y disposición de registros e información.
- Elaborar un programa de retención que identifique los registros y el período de tiempo durante el cual se deberían retener, de acuerdo con lo definido en las tablas de retención definidas por Gestión documental
- Llevar un inventario de fuentes de información clave.

Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.

Desarrollar e implementar una política relativa a datos del MEN, para la privacidad y la protección de datos personales. Esta política se debe comunicar a todas las personas involucradas en el procesamiento de información de datos personales.

Usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación reglamentación pertinentes.

Considerar los siguientes aspectos en relación con la conformidad con los acuerdos, leyes y reglamentaciones de la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA:

- las restricciones sobre importación o exportación de hardware y software informático, para la realización de funciones criptográficas;
- las restricciones sobre importación o exportación de hardware y software informático que está diseñado para la adición de funciones criptográficas;
- las restricciones sobre el uso de la encriptación;
- los métodos obligatorios o discrecionales de acceso por parte de las autoridades de los países a información encriptada mediante software o hardware para brindar confidencialidad al contenido.

Revisar independientemente a intervalos planificados o cuando ocurran cambios significativos, el enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información).

Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.

Revisar periódicamente los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Revisar periódicamente, mínimo una vez al año, los sistemas de información para determinar el cumplimiento de las políticas y normas de seguridad de la información.

Revisar preferiblemente con la ayuda de herramientas automáticas que generan informes técnicos para la interpretación posterior por un especialista técnico. Como alternativa, un ingeniero de sistemas experimentado puede llevar a cabo revisiones manuales (si es necesario, con el apoyo de herramientas de software apropiadas).

Si se usan pruebas de penetración o valoraciones de vulnerabilidad, es necesario tener precaución, ya que estas actividades pueden comprometer la seguridad del sistema. Estas pruebas se deben planificar, documentar, y deben ser repetibles.

Cualquier revisión de cumplimiento técnico solo podrá ser llevada a cabo por personas competentes autorizadas, o ser realizada bajo la supervisión de dichas personas.

RESPONSABILIDAD

Empleados y contratistas vinculados con la DIRECCIÓN DE TRÁNSITO DE BUCARAMANGA.

RESULTADO CLAVE

Dar cumplimiento a la política de requerimientos legales y contractuales.