INTRODUCCIÓN

Alcanos de Colombia S.A. E.S.P.a reconoce la importancia que tiene la información y, que esta constituye uno de los activos más valiosos que exige ser protegido de los riesgos que atentan contra su disponibilidad, integridad y confidencialidad. Así mismo, es consciente de las amenazas a las que están expuestos sus activos de información e infraestructura soportada en las tecnologías de información y comunicaciones (TIC), y de las consecuencias que estas pueden traer sí la compañía no establece e implementa los niveles de protección y respuesta apropiados.

Por lo anterior, es necesario realizar una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riesgos de seguridad que puedan afectar la información de la compañía, con el objetivo de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

La presente Política de Seguridad de la Información tiene como propósito establecer los principios, lineamientos y procedimientos que enmarcan la actuación de todos los empleados y contratistas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la organización y partes interesadas, y como tal se establece para su estricto cumplimiento.

1 GENERALIDADES:

1.1 Objetivo General

Facilitar y proporcionar una guía de acción para el uso adecuado de la infraestructura tecnológica corporativa, incluyendo aspectos organizacionales, técnicos, físicos y legales que contribuyan a proteger y salvaguardar los activos de información de la Compañía.

1.2 Alcance

La operación de **Alcanos de Colombia S.A. E.S.P.** se soporta en una infraestructura tecnológica conformada por redes de datos, hardware, sistemas de información y recursos informáticos, esta política, aplicable a todos los funcionarios directos, indirectos o terceros que hagan uso de los activos de información de la Compañía, contiene estándares, mejores prácticas, guías y procedimientos que permiten hacer un uso efectivo y adecuado de los activos de información garantizando su confidencialidad, integridad y disponibilidad.

1.3 Documentos Relacionados

INST – 05-007 POLITICAS PARA LA RADICACIÓN Y GESTIÓN DE REQUERIMIENTOS.

INST – 02-002 POLÍTICA DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES.

DEA – 16-003 POLÍTICA DE GESTIÓN HUMANA.

1.4 Dirección de la Política

- Responsabilidad

Es responsabilidad del área de TI definir los estándares, procedimientos y lineamientos que garanticen el cumplimiento de la política de seguridad de la información

- Cumplimiento

El cumplimiento de la política de seguridad de la información es obligatorio para todos los funcionarios directos, indirectos o terceros que hagan uso de los activos de información de la Compañía. De presentarse una violación a la política, **Alcanos de Colombia S.A. E.S.P.** se reserva el derecho de tomar las acciones correspondientes.

- Excepciones

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deben ser aprobadas por el área de TI y la Gerencia General. Las excepciones deberán ser documentadas formalmente.

1.5 Definiciones

Acceso: Es la respuesta positiva de una autenticación.

Activo de información: Cualquier cosa que tenga valor para la empresa. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización.

Administración de riesgos: Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.

Archivos adjuntos: Son archivos que se envían junto a un correo electrónico.

Archivo log: Archivo de grabación secuencial de todos los acontecimientos en una base de datos que afectan en un proceso particular.

Ataque por Injection: También conocido como Inyección SQL, es una vulnerabilidad que permite al atacante enviar o "inyectar" instrucciones SQL de forma maliciosa y malintencionada dentro del código SQL programado para la manipulación de bases de datos

Autenticación: Es la acción o proceso de confirmación que un usuario o dispositivo es quien dice ser.

Backup: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

BAT: Contiene procesamiento por lotes, es decir, instrucciones de MS-DOS.

Buzón de correo electrónico: Es la recolección de todos los mensajes que el usuario ha enviado y recibido desde y hacia su dirección de correo electrónico.

Cifrado: Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje.

COM: Es un tipo de archivo simple ejecutable.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. El activo debe ser accedido únicamente por el recurso autorizado

Control: Es una medida implementada que permite salvaguardar que permite reducir el nivel del riesgo u ofrecer mejorar al negocio.

CPU: (Central Processing Unit) unidad central de procesamiento, interpreta las instrucciones de un programa informático

Dato: Representa de forma simbólica un atributo o variable cualitativa o cuantitativa.

Datacenter: Denominado Centro de Datos, es el espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Datagrama: Es un paquete de datos que constituye el mínimo bloque de información en una red de conmutación

Defacement: Es un ataque a un sitio web que cambia la apariencia visual de una página Web.

Derechos de autor: Hace referencia a un conjunto de normas jurídicas y principios que afirman los derechos morales y patrimoniales que se otorga a los autores, por la creación de obras científicas, literaria, artística, entre otras

Desastre: Interrupción de la capacidad de acceso a información y procesamiento de esta a través de computadoras u otros medios necesarios para la operación normal de un negocio

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Dispositivo móvil: Es un tipo de computador pequeño, con capacidad de procesamiento, con conectividad, con memoria interna, que permite cumplir una función específica.

DLL: (Dynamic Enlace Library). Son bibliotecas de controladores requeridas por aplicaciones integradas de Windows y programas de terceros que han sido desarrollados para Microsoft Windows.

DNS: (Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

Estándares de seguridad: son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

EXE: (Executable). Se refiere a un archivo ejecutable, cuyo contenido permite instalar una aplicación dentro de un equipo de cómputo.

Extensión: Permite identificar el tipo de archivo, de tal forma que el sistema operativo disponga del proceso necesario para ejecutarlo o interpretarlo.

Firewall: Es el componente dentro de un sistema de información o una red que permite bloquear el acceso no autorizado a usuarios o algún componente tecnológico.

Hardware: Hace referencia a todos los componentes físicos que hace parte de un computador u componente tecnológico dentro de una red.

HTTP: (Hypertext Transfer Protocol) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

Impacto: Es la consecuencia sobre un activo de la materialización de una amenaza.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: propiedad de salvaguardar la exactitud y el estado completo de los activos. El activo debe ser modificado únicamente por el recurso autorizado.

Intérprete: Son programas informáticos que permiten analizar y ejecutar programas.

IP: es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado.
ISP: (Internet Service Provider) empresa que brinda conexión a internet a sus clientes.

KEYLOGGER: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Lenguaje de programación: Es un lenguaje que le permite al programador escribir una serie de instrucciones u órdenes que permiten construir un programa.

Malware: Conocido también como Malicious Software, programa malicioso, programa maligno, código maligno, software maligno, software dañino o software malintencionado a cualquier tipo de software que ejecuta tareas dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Medios magnéticos: Son dispositivos de almacenamiento de datos como discos duros, CD-ROM o DVD-ROM.

Mesa de ayuda: Conjunto de recursos tecnológicos y humanos que prestan servicio de gestión y solución de posibles incidencias que se presenten.

Microsoft: Es una multinacional compañía tecnológica. Conocida por el desarrollo de productos como MS-DOS, Windows y Office.

MMS: (Multimedia Messaging Service) Servicio de mensajería multimedia. Permite a los teléfonos móviles enviar y recibir archivos multimedia como fotos, videos y sonido.

MS-DOS: Primer sistema operativo de Microsoft.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación

de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Políticas: Toda intención y directriz expresada formalmente por la dirección.

Probabilidad: Corresponde a la probabilidad existente de que una amenaza afecte a un determinado activo aprovechando la vulnerabilidad que esté presente en él.

Ransonware: Un ransomware, o "secuestro de datos" en español, es un tipo de programa dañino que aplica restricciones de acceso a determinadas secciones o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Riesgo: Es la posibilidad que se produzca un impacto sobre algún activo.

Roles de acceso: Hace referencia a los derechos de ingreso de un usuario a un sistema de información, equipo de cómputo o dispositivo tecnológico que requiera autenticación.

Script: Se considera como un conjunto secuencial de comandos, son ejecutados por un intérptrete.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SMS: (Short Message Service) Servicio de mensajes cortos. Los teléfonos móviles pueden realizar envío de mensajes cortos con un límite de caracteres.

Software: Son los programas informáticos que permiten al usuario realizar tareas específicas.

SysAid: Aplicativo de gestión de tickets.

Syn Flood: Es un tipo de ataque de denegación de servicio (DdoS) que busca dejar un servidor sin disponibilidad para el tráfico legítimo ya que consume todos los recursos disponibles del servidor.

TCP/IP: Es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red.

TI: Tecnologías de la información.

UDP: (User Datagram Protocol) se utiliza para transmitir datagramas de forma rápida en redes IP y funciona como una alternativa sencilla y sin retardos del protocolo TCP.

Usuario: Es la persona que utiliza un equipo de cómputo, un sistema de información o un servicio de red.

Virus: Es un software cuyo objetivo es afectar de forma malintencionada el funcionamiento adecuado de un sistema informático.

VBS: Archivos de Script de Visual Basic.

Visual Basic: Es un lenguaje de programación dirigido a eventos.

VPN: (Virtual Privated Network) – Red privada virtual, permite tener una extensión segura de una red de área local (LAN).

Vulnerabilidad: Es la posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

Web: Significa red informática.

Wiping: Hace referencia a limpiar.

Zeroing: Puesta a cero.

2 LINEAMIENTO NORMATIVO

- Norma ISO/IEC 27001 Seguridad de la Información

3 POLÍTICAS Y PROCEDIMIENTOS

3.1 Política de Organización de Seguridad de la Información

3.1.1 El área de TI es responsable de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en Alcanos de Colombia S.A. E.S.P.

La política de seguridad tiene por objetivo aportar las directrices de la seguridad de la información de acuerdo con los requerimientos específicos de la organización y con la legislación vigente. La información es un activo esencial para las actividades de la Compañía y por consiguiente debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad.

A través de esta Política se dan a conocer los objetivos de seguridad de la información de **Alcanos de Colombia S.A. E.S.P.** que se consiguen con la aplicación de controles de seguridad para gestionar un nivel de riesgo aceptable. Con esto se busca minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos de negocio y de las obligaciones legales conforme al marco jurídico vigente, señalando los estándares, reglas y medidas de seguridad que va a adoptar la organización para impedir infracciones y violaciones de seguridad a la información.

3.1.2 Estándares De La Política De Organización De Seguridad De La Información

Responsabilidades para la seguridad de la información. Alcanos de Colombia S.A. E.S.P. es el propietario de la información. Su tenencia y manejo es delegada a las Direcciones y Jefaturas de área de la compañía, quienes son responsables de la custodia de la información generada, considerando su propósito y uso. De acuerdo con esto, deben ser conscientes de los riesgos a la que está expuesta la información a su cargo, y por tanto ejercer, frente a sus colaboradores el liderazgo apropiado para disminuirlos.

Contacto con autoridades y grupos de interés. Alcanos de Colombia debe mantener contacto con las autoridades y grupos de interés para estar al corriente en cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información.

3.2 Política de Clasificación y Control de Activos de Información

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la compañía, la información deberá estar clasificada en niveles de confidencialidad. La información con los dos niveles más altos debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

3.2.1 Estándares de la Política de Clasificación y Control de Activos de Información

Metodología de clasificación de los activos. Para asegurar que los activos de información reciben el nivel de protección adecuado, el área de TI es responsable de definir la metodología de clasificación de activos de información.

Identificación de activos de información. Se denominan Activos de Información a todos aquellos recursos de valor para **Alcanos de Colombia S.A. E.S.P.** que generan, procesan, almacenan o transmiten información.

Clasificación de activos de información. Se define la criticidad de un activo en función de cuán necesario resulta para las actividades de un área o la misión de la organización. Dado que no todos los activos de información poseen el mismo valor, a la vez que un mismo activo puede poseer un valor diferente para distintas áreas, se establece una valoración estandarizada donde se clasifica cada activo según las tres características básicas de la seguridad de la información: la confidencialidad, la integridad, y la disponibilidad a la que debe estar sometido.

Responsabilidad. Alcanos de Colombia S.A. E.S.P. pone al servicio de sus colaboradores el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

3.3 Política de Uso Aceptable de los Activos de Información

Todos los colaboradores, consultores, contratistas y terceros, que usen activos de información que sean propiedad de **Alcanos de Colombia S.A. E.S.P.**, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable para dar un uso racional y eficiente a los recursos asignados.

3.3.1 Estándares para el Uso Aceptable de los Activos de Información

Uso de los sistemas de información y equipos de cómputo. La Compañía hace uso del inicio de sesión en los equipos de cómputo para notificar sobre la política de uso aceptable de los sistemas y equipos de cómputo.

*"¡Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida, es propiedad de **Alcanos de Colombia S.A. E.S.P.** y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de este sistema implica su consentimiento con esta política."*

Correo electrónico. La compañía, como muestra del respeto por los principios de libertad de expresión y privacidad de información, advierte a sus colaboradores que no generará ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico corporativo propiedad de **Alcanos de Colombia S.A. E.S.P.**; en consecuencia, podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado. Sin embargo, no se realizará monitoreo o inspección en un buzón de correo electrónico corporativo sin el conocimiento del colaborador que tenga a cargo la administración del buzón, salvo autorización de la Gerencia General para casos que incluye, pero no se limitan a:

- Requerimiento legal.
- Sospecha de violación de las políticas internas de la Compañía o de leyes nacionales.
- Por circunstancias de emergencia en las cuales el no actuar repercuta gravemente en el desarrollo del objeto de la Compañía.
- La desvinculación laboral del colaborador con la Compañía.

En estos casos la Compañía puede inspeccionar y cerrar el buzón de correo o hacer un backup de la información para prevenir su pérdida o adulteración.

La cuenta de correo electrónico corporativo debe utilizarse solo para tareas y objetivos organizacionales y no para fines particulares. Las comunicaciones por correo electrónico entre la Compañía y sus públicos de interés deben hacerse a través del correo corporativo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, ni para transmitir cualquier otro tipo de información del negocio.

A los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, el área de TI se la asigna previo requerimiento del jefe inmediato, radicado en la mesa de ayuda. De igual manera, el correo corporativo será suspendido una vez el área de Gestión Humana informe a través del paz y salvo el retiro de los colaboradores.

Cada cuenta de correo electrónico corporativo cuenta con una cuota de capacidad máxima para almacenamiento.

La plataforma de correo corporativo de la Compañía filtrará los archivos adjuntos a los mensajes de correo electrónico para verificar la ausencia de virus, por lo que la entrega efectiva estará sujeta a esta comprobación.

El buzón de correo es personal e intransferible y corresponde al colaborador o grupo de funcionarios a cargo (para casos de buzones de correo compartidos) velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la organización, el usuario se compromete a:

- Respetar la privacidad de las cuentas de otros colaboradores, tanto dentro como fuera de la red corporativa. El usuario del correo no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.

- El colaborador titular del correo asignado por la organización usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo. En su uso el colaborador actuará siempre con respeto y cortesía, no está permitido el envío de información con intención de hostigar, irrespetar a otros, difamar u ofender, al igual que comunicaciones tipo cadena, pornografía, información obscena, venta de productos o servicios que no sean de la Compañía y mensajes de índole político o religioso.

- Para dar respuesta sobre un mismo correo electrónico estar seguro de mantener la trazabilidad de este de igual forma escoger el(los) usuario(s) destino correctamente, observar los archivos adjuntos recibidos y escoger los adecuados para enviar ya que se puede exponer información sensible y confidencial a personas sin autorización.

- Los colaboradores de la Compañía se abstendrán de utilizar la cuenta para el envío o reenvío de

mensajes spam (correos no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), (es un intento de hacer creer que algo falso es real a través de un medio electrónico), con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía), o que sea contrario a las políticas y normas institucionales.*hoax*

- Evitar el envío desde su buzón de elementos (textos, software, música, imágenes o cualquier otro con extensión .EXE, .DLL, .COM, .BAT y .VBS) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. Está prohibida la distribución de software que requiera licencia, claves ilegales de software, programas para romper licencias (crackers), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. Dentro de los elementos por razones de seguridad se prohíbe

- Solo si es estrictamente necesario envíe un correo a toda la Compañía (lista **alcanos_de_colombia@alcanosesp.com**) y en caso de recibir uno, no utilice la opción responder a todos, la respuesta solo debe ir dirigida a la dirección de correo que envió originalmente el mensaje, salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos.

- Es responsabilidad de quien tiene a cargo el buzón de correo corporativo realizar mantenimiento periódico de su cuenta cuando el sistema le haga advertencias de espacio disponible. Es importante evitar que mensajes innecesarios permanezcan en el buzón un tiempo excesivo causando congestión o bloqueo de este.

- Los colaboradores con cuenta de correo corporativa no deben usar su cuenta como una herramienta de mensajería instantánea. Todos los mensajes podrán ser tenidos en cuenta como proceso probatorio ante la ley colombiana.

- **Mensajería instantánea y redes sociales**

El chat es una herramienta de comunicación provista por la Compañía para apoyar las funciones desempeñadas por cada colaborador. Está habilitado para todos los funcionarios que tengan una cuenta de correo corporativa y debe ser utilizado solo para actividades y objetivos organizacionales. Al igual que un correo electrónico se deben guardar las normas de respeto y cortesía. No está permitido el envío de mensajes con intención de hostigar, irrespetar, difamar u ofender, así mismo la transmisión de información obscena y mensajes de índole político o religioso.

El acceso a redes sociales estará autorizado solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con los clientes de la Compañía.

- **Navegación en Internet**

El uso de Internet está destinado exclusivamente a la ejecución de las actividades de la organización y debe ser utilizado por el colaborador para realizar las funciones establecidas para su cargo, de acuerdo con los siguientes parámetros de uso:

- El colaborador debe abstenerse de descargar y/o utilizar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.

- La descarga de música y videos no es una práctica permitida.

- Las salas de video-conferencia de la Compañía deben ser de uso exclusivo para asuntos laborales. Cualquier excepción a esta política debe ser autorizada por Gerencia General o Gerencia del Centro Operativo.

- No está permitido el uso de sitios que salten la seguridad de navegación dispuesta por la Compañía (proxy).

- Los colaboradores no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona o institución.

- Los colaboradores no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la ley o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier ley estatal, local, nacional o internacional; incluyendo, pero no limitado, las leyes y regulaciones de control de Colombia y los decretos sobre fraudes

de computación.

- Los colaboradores se deben abstener de coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos, expedientes o programas.

- Los colaboradores deben abstenerse de publicar información propia de **Alcanos de Colombia S.A. E.S.P.** en redes sociales, plataformas de publicación de documentos sin autorización.

- Uso de herramientas que comprometen la seguridad

No está permitido el uso de herramientas que comprometen la seguridad, así como hacer o intentar dicha acción sin autorización de la jefatura del área de TI, cualquiera de los siguientes actos:

- Acceder al sistema o red.

- Monitorear datos o tráfico.

- Sondear, copiar, probar firewalls o herramientas de hacking.

- Atentar contra la vulnerabilidad del sistema o redes.

- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

- Unidades de red

Cada usuario cuenta con un espacio de almacenamiento en la red de la Compañía, este espacio está destinado para almacenar toda la información propia de las actividades del cargo desempeñado por el usuario, la configuración del almacenamiento por defecto en esta ubicación es responsabilidad del área de TI, sin embargo es responsabilidad del usuario informar a través de la mesa de ayuda cualquier advertencia o novedad que el sistema informe acerca de la disponibilidad de la unidad de red o su proceso de sincronización.

No está permitido el almacenamiento de información personal incluyendo música y vídeos en las unidades de red. La Compañía ha incluido dentro de su esquema de copias de seguridad los datos almacenados en las unidades de red.

- Almacenamiento

Las unidades de almacenamiento con que cuenten los equipos de cómputo asignados por la compañía a sus colaboradores solo deben ser utilizadas para almacenar información propia de las actividades del cargo desempeñado por el funcionario. La Compañía se reserva el derecho a eliminar cualquier otro tipo de información que no corresponda a actividades laborales y no estará obligada a la realización de copias de seguridad de esta información.

- Uso equipos portátiles y dispositivos móviles

Los colaboradores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la Compañía, tales como aplicaciones, escritorios y aplicaciones virtuales, correo electrónico, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

- Uso de aplicación de antivirus.

- Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.

- No abrir o aceptar mensajes de correo electrónico, SMS, MMS entre otros que vengan de origen desconocido.

- Mantener actualizado el sistema operativo de su dispositivo móvil, con las últimas actualizaciones disponibles previniendo que el dispositivo móvil sea expuesto a posibles vulnerabilidades.

- Evitar tener conexión a redes no seguras o no conocidas.

- Contar con la configuración de algún patrón de seguridad para el bloqueo del dispositivo móvil.

El área de TI debe implementar las acciones necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se compromete la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos. Para esto se establecen los mecanismos adecuados para control del acceso.

3.4 Política de Análisis y Gestión del Riesgo

El análisis de riesgos en pro de la seguridad de la información es responsabilidad del área de TI, con base en los objetivos de negocio y para los activos de información que se encuentren bajo su custodia.

3.4.1 Estándares para el Análisis y Gestión del Riesgo

La gestión de riesgos se presenta como una actividad clave para el resguardo de los activos de información de la organización y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riesgos que presentan los activos de información a niveles aceptables para la misma.

El proceso de gestión de riesgos involucra cuatro actividades cíclicas:

- La identificación de activos y los riesgos a los que están expuestos.
- El análisis de los riesgos identificados para cada activo.
- La selección e implantación de controles que reduzcan los riesgos.
- El seguimiento, medición y mejora de las medidas implementadas.

3.5 Política de Seguridad Vinculada al Personal

El área de Gestión Humana debe notificar al área de TI todas las novedades del personal directo e indirecto relacionadas con ingresos, traslados, retiros y vacaciones.

3.5.1 Estándares para la Seguridad Vinculada al Personal

- **Seguridad anterior a la contratación**

El área de Gestión Humana debe asegurar que las responsabilidades sobre los activos de información a los que tendrá acceso el funcionario durante el desarrollo de sus labores estén explícitas y se reflejen apropiadamente en los manuales de funciones del cargo y los términos y condiciones de contratación.

- Seguridad en la contratación

El área de Gestión Humana debe asegurar que todos los colaboradores directos o indirectos que ingresen a la Compañía o cambien de cargo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que **Alcanos de Colombia S.A. E.S.P.** lo considere conveniente, incluyendo un periodo de tiempo posterior a la finalización de la relación contractual.

- Seguridad en la finalización de la contratación

El área de Gestión Humana a través de la apertura del paz y salvo informará al área de TI la terminación de la relación contractual con el funcionario, de tal forma que se deshabiliten los accesos que correspondan a los sistemas de información y medios de conexión y comunicación que tenía disponibles el funcionario y se valide la devolución de todos los activos de información que tenía a cargo.

- Responsabilidad sobre los activos de información

Los recursos tecnológicos y de software que **Alcanos de Colombia S.A. E.S.P.** asigna a los funcionarios son responsabilidad de cada uno y solo deben ser utilizados para los fines autorizados por la Compañía.

3.6 Reporte de Incidentes de Seguridad

Con el fin de establecer acciones y lineamientos, que permita a **Alcanos de Colombia S.A. E.S.P.**, no solo estar en capacidad de responder en forma adecuada ante la ocurrencia de incidentes de seguridad que afecten real o potencialmente sus servicios, sino también establecer la forma como pueden ser detectados y evaluados junto con la gestión de vulnerabilidades, asegurando que los sistemas, redes y aplicaciones sean lo suficiente seguros. Para ello, se debe:

- Gestionar los eventos de seguridad de información de acuerdo con los roles y responsabilidades definidos para detectar y tratar con eficiencia.
- Poder identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.

- Minimizar los impactos adversos de los incidentes en la compañía y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.

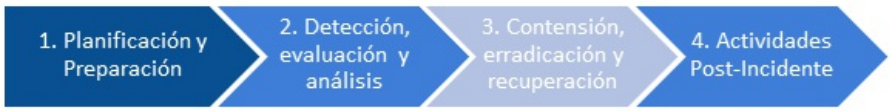
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.

- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.

- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.

- Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.

El proceso para gestión de incidentes estaría enmarcado dentro de lo siguiente:



1. disponer de los responsables involucrados, podrían ser usuarios finales, administrador de infraestructura, Jefe de sistemas, etc. Tener acceso a la herramienta SysAid para poder realizar el reporte del incidente.

2. las principales fuentes de detección de incidentes son los usuarios y el monitoreo de la infraestructura.

Reporte de usuarios:

Los usuarios de los diferentes servicios informáticos, sistemas de información y aplicaciones de **Alcanos de Colombia S.A. E.S.P.** deben reportar el incidente por medio de la herramienta SysAid permitiendo:

-Especificar la descripción detallada del incidente.

-Adjuntar archivos como evidencias.

-Conocer el estado del incidente reportado.

-Responsable de la solución del incidente.

Monitoreo de infraestructura:

El área de TI debe realizar revisión continua del funcionamiento de los activos de información, para prevenir problemas, eventos no deseados e incidentes de seguridad de la información.

Es necesario contar con una serie de elementos indicadores que alerten que posiblemente ha ocurrido un incidente:

-Alertas en Sistemas de Seguridad

-Caídas de servidores

-Reportes de usuarios

-Informe Software antivirus

-Funcionamiento de los sistemas fuera de lo normal

-Tráfico de red excepcionalmente intenso

-Falta de espacio en el disco, o reducción considerable del espacio libre

-Utilización excepcionalmente alta de la CPU

-Creación de nuevas cuentas de usuario

-Uso o intento de uso de cuentas de administrador

-Cuentas bloqueadas

-Gran número de correos electrónicos rebotados con contenido sospechoso

El área de TI, debe aplicar las siguientes actividades con el fin de garantizar la detección de incidentes de seguridad:

- Verificar la utilidad de Administración (Visor de Eventos) del sistema operativo de cada equipo Servidor que hacen parte del Datacenter.

- Activar el módulo de auditoria del Gestor Base de Datos de los sistemas de información y/o aplicaciones corporativas.

- Realizar acciones correctivas sobre los sucesos registrados

- Verificar la operatividad y funcionabilidad acciones plan de contingencia (Restauración de backup).

- Verificar la eficacia de los planes de mejoramiento.

Una vez se detecta el incidente, ya sea por parte del usuario final o del administrador del sistema, se genera un reporte del incidente en SysAid

Análisis: dentro de las actividades se involucran los siguientes componentes a tener en cuenta:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.

- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.

- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).

- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.

- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.

- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.

- Determinar el alcance, las posibles consecuencias e impactos del incidente de seguridad en cuanto al desarrollo de los procesos, la confidencialidad, integridad y disponibilidad de la información, daños físicos a la infraestructura tecnológica y la percepción pública.

- Determinar la naturaleza del incidente en lo que respecta a la intención del atacante y a la amenaza existente.

- Determinar la causa raíz del incidente y establecer los controles y procedimientos para prevenir o mitigar su repetición en el futuro.

- Identificar la fuente del ataque y el atacante, y elaborar un perfil de este.

Evaluación: en la realización de la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad.

La severidad del incidente puede ser:

Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de la compañía. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

Medio Impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

Priorización de los incidentes de seguridad y tiempos de respuesta

Cuando se conozca la incidencia, se continúa con la priorización de acuerdo con el impacto y posibles consecuencias que atenten contra la continuidad de los procesos de los objetivos de la compañía.

El área de TI, una vez tiene conocimiento del incidente, procede a realizar la verificación, análisis y evaluación de este y establece niveles de prioridad de acuerdo con el tipo de incidente y complejidad en las acciones de respuesta.

El nivel de prioridad depende de la importancia o valor dentro de **Alcanos de Colombia S.A. E.S.P.**

Nivel de criticidad	Valor	Descripción
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola Dependencia o proceso de la compañía.
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso de la compañía.
Alto	0,75	Sistemas pertenecientes al área de tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas Críticos. La operación es crítica para la compañía cuando al no contar con ésta, la función del proceso no puede realizarse.

Tabla: Niveles de criticidad del impacto

Impacto actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Nivel de criticidad	Valor	Descripción
Inferior	0,10	Impacto no significativo en uno de los componentes de cualquier Sistema de Información o estación de trabajo.
Bajo	0,25	Impacto leve en uno de los componentes de cualquier Sistema de Información o estación de trabajo.
Medio	0,50	Impacto moderado en uno de los componentes de cualquier Sistema de Información o estación de trabajo.
Alto	0,75	Impacto considerable en uno o más componentes de más de un Sistema de Información.
Superior	1,00	Impacto muy alto en uno o más componentes de un Sistema de Información.

Tabla: Niveles de Impacto Actual y Futuro

*Nivel de Prioridad= (Impacto actual*2,5) + (Impacto futuro *2,5) + (criticidad del*

*sistema *5)*

Y el resultado se compara con la siguiente tabla para determinar el nivel de prioridad de atención:

Nivel de Prioridad	Valor
Inferior	00,00 - 02,49
Bajo	02,50 - 03,74
Medio	03,75 - 04,99
Alto	05,00 - 07, 49
Superior	07,50 - 10, 00

Tabla: Niveles de prioridad del incidente

Tiempos de respuesta

El tiempo de respuesta establecido en la siguiente tabla es aproximado al tiempo máximo para que el incidente sea atendido dependiendo del nivel de prioridad, y no corresponde al tiempo de solución del incidente, dado que la complejidad de la atención varía dependiendo del tipo de incidente y del activo de información impactado.

Nivel de Prioridad	Tiempo de respuesta
Inferior	6 horas
Bajo	3 hora
Medio	60 minutos
Alto	30 minutos
Superior	15 minutos

Tabla: Tiempos máximos de respuesta

Qué hacer	Cómo hacerlo	Quién lo hace	Cuando lo hace
Notificación o reporte del incidente	Por medio de la herramienta SysAid. administrador.sistemas@alcanosesp.com coordinador.soporte.ti@alcanosesp.com	Usuario, tercero o contratista, o Administrador TI	Inmediatamente tenga conocimiento del incidente.
Registro del incidente o evento	Toma los datos necesarios y realiza el registro en la herramienta SysAid, si se puede solucionar de inmediato se documenta la solución aplicada entre otros.	Primer punto de contacto Administrador TI	En el momento del reporte del incidente o evento.
Identificar el tipo de incidente	Identificación del tipo de incidente, verificar las evidencias, realizar pruebas determinando la veracidad de la incidencia, las causas y el impacto.	Primer punto de contacto Administrador TI	Inmediatamente a la herramienta de mesa de ayuda y según la tabla de tiempos de respuesta.
Escalar el incidente	Se debe asignar a la persona encargada de dar atención al incidente para que tome las decisiones correspondientes.	Primer punto de contacto Administrador TI	Inmediatamente a la herramienta de mesa de ayuda y según la tabla de tiempos de respuesta.
	Para recolectar la evidencia tener en cuenta lo siguientes criterios: - **Información basada en la red:** Log's de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de		

Recolectar la evidencia	servidores de autenticación. -**Información Basada en el Equipo:** Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. -**Otra información:** Ticket reportado en la herramienta de mesa de ayuda por parte del funcionario o contratista que reporta el evento o incidente.	Profesionales y técnicos del área de TI, Administrador TI	Desde el conocimiento del incidente.
Manejo de la Evidencia	La información debe ser almacenada y custodiada, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. Esta información debe incluir: -Cantidad de incidentes presentados y tratados. -Tiempo asignado a los incidentes. -Daños ocasionados. -Vulnerabilidades explotadas. -Cantidad de activos de información involucrados. -Frecuencias de ataques. -Pérdidas.	Administrador TI	Al cierre del proceso.
Evaluar el impacto	Evaluar el impacto del incidente en la infraestructura tecnológica y en el desarrollo de los procesos de la compañía. Cuando el impacto sea superior que ponga en riesgo la estabilidad, seguridad y resiliencia del sistema, se informa al Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional.	Administrador TI.	Según la tabla de tiempos de respuesta.
Delegar responsabilidades	Asignar las acciones de erradicación de la incidencia al personal del grupo del área TI dependiendo de la competencia.	Jefe TI	Durante las doce horas siguientes al reporte de la evaluación del impacto.
Verificar existencia de recursos	Verificar la disponibilidad de recursos necesarios para la recuperación tales como manuales, backups de sistemas operativos, aplicativos, bases de datos, antivirus, equipos, sistemas eléctricos, servicios de internet y de correo.	Profesionales y técnicos del área de TI, Administrador TI	Inmediatamente después de la delegación.
	Asignar los recursos físicos, tecnológicos,		Durante las doce horas siguientes

Disponer de la logística	comunicaciones, transporte y demás necesarios para la ejecución del plan de recuperación.	Jefe TI	al reporte de la evaluación del impacto.
Comunicar a los usuarios	Informar a los usuarios del proceso a intervenir, indicando el tiempo probable de suspensión del sistema, el cual dependen del nivel de complejidad del incidente, previamente establecido en el procedimiento.	Administrador TI	Una vez de conozca la disponibilidad de recursos.
Aplicar la estrategia de recuperación	Realizar las acciones de la estrategia de recuperación (tabla de clasificación y estrategias de respuesta).	Profesionales y técnicos del área de TI, Administrador TI	Según la tabla de tiempos de respuesta.
Comunicar el restablecimiento del servicio	Informar a los usuarios la puesta en marcha del sistema.	Administrador TI	Inmediatamente a la terminación de las acciones de restauración.
Pruebas	Monitorear el comportamiento del sistema durante tres horas y se deja registrado en la herramienta de mesa de ayuda.	Administrador TI	Inmediatamente a la terminación de las acciones de recuperación.
Retroalimentación	Se aplica una encuesta sobre el funcionamiento del sistema o del Hardware.	Administrador TI	Inmediatamente a la terminación de las pruebas.
Cerrar el proceso	Presentar un informe del incidente, de las acciones de respuesta aplicadas o acciones correctivas, proponer las acciones preventivas y de mejora para evitar reincidencias.	Primer punto de contacto Administrador TI	Posterior a las pruebas a satisfacción.

3. Para evitar la propagación del incidente, disminuir el impacto sobre los activos de información, y garantizar la confidencialidad, integridad y disponibilidad de la información, en **Alcanos de Colombia S.A. E.S.P.**, se establecen las siguientes actividades:

Contención: busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.

Una vez se apliquen las estrategias de contención, se procede a la recolección de la evidencia, para lo cual se debe tener en cuenta:

- **Autenticidad:** El usuario recolector de las evidencias debe poder probar que son auténticas.

- **Cadena de Custodia:** Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, con tal fin de evitar alteraciones o modificaciones que comprometan la misma.

- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante los entes de control.

Durante el proceso de recolección de evidencias es importante considerar realizar las siguientes acciones:

- Registrar información que rodea a la evidencia.

- Tomar fotografías del entorno de la evidencia.

- Tomar la evidencia.

- Registrar la evidencia.

- Rotular todos los medios que serán tomados como evidencia.

- Almacenar toda la evidencia de forma segura.

- Generar copias de seguridad de la evidencia original.

- Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada.

Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el Administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita

prevenir incidentes similares en el futuro.

CLASIFICACION Y TRATAMIENTO DE INCIDENTES			
Clase de incidente	**Concepto**	**Tipo de Incidente**	**Tratamiento**
Denegación del servicio	Estos incidentes hacen que un sistema, servicio o red dejen de operar a su capacidad prevista y con mucha frecuencia deja sin acceso a usuarios legítimos del sistema o servicio tecnológico afectado. Existen dos tipos de incidentes DoS/DDoS causados por medios técnicos: eliminación y agotamiento de recursos. DoS: son aquellos causados porque el número de peticiones lanzado desde un equipo cliente a un servidor excede el límite permitido y ello causa que el servidor afectado deje de estar disponible. DDoS: varios equipos haciendo peticiones a un mismo servidor. El ciberataque busca desconectar el sitio web o al menos hacerlo tan lento que los visitantes dejen de intentar usarlo. Esto se logra saturando el sitio web con tráfico malicioso, ya sea dirigido a la red o al servidor. (Inundación UDP, DNS, HTTP,SYN FLOOD).	- Tiempo de respuesta fuera del normal. - Interrupción de servicios tecnológicos. - Envío masivo de miles mensajes de correo electrónico (“mail bombing”), provocando la sobrecarga del servidor de correo y/o de las redes afectadas. - SYN FLOOD. - Ataque a través de equipo Zombis. - Ataque contra algunos sistemas de Windows para disminuir su rendimiento - Activación programas bacterias para consumir la memoria y la capacidad del procesador. - Error Humano.	**Contención** -Bloquear o redirigir los paquetes del ataque. -Buscar nuevos canales de comunicación entre el servicio y sus usuarios. -Detener las IPs Invalidas. -Terminar conexiones o procesos no deseados en servidores y enrutadores y sintonizar sus configuraciones TCP / IP. -Testing de servidor. **Erradicación** -Involucrar el proveedor de ISP, - Filtrado. -Restitución del servicio caído. **Recuperación** üVolver el servicio al estado original.
	Consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red. Es un incidente que involucra a	- Intentos reiterativos de acceso a recursos. - Ataque de fuerza Bruta - Captura de cuentas de usuario y contraseña mediante herramientas como el KEYLOGGERS. - Divulgación no autorizada de información personal.	**Contención** -Apagado del Sistema. -Bloqueo de la cuenta. **Erradicación** -Implementar bloqueos automáticos por exceso de intentos. -Cambio de contraseñas. -Uso de contraseñas seguras. -Determinar los puntos de

Acceso no autorizado	una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.	- Intrusión física a las instalaciones. - Consultas no autorizadas. - Intento de acceso no autorizado a base de datos. - Acceso no autorizado a carpetas privadas. - Creación de usuarios sin autorización.	acceso usados por el atacante e implementar las medidas adecuadas para evitar futuros accesos. -Las medidas pueden deshabilitar un módem. -Control de acceso en el firewall. -Aumento de las medidas de seguridad físicas. **Recuperación** -Activar las cuentas de usuario. -Habilitar el sistema.
Modificación de Recurso no Autorizado	Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.	- Borrado de Información. - Modificación de información. - Modificación, instalación o eliminación no autorizada de software.	**Contención** -Bloqueo de la cuenta. **Erradicación** -Corrección de efectos producidos. -Sustitución de los archivos comprometidos con versiones limpias. **Recuperación** -Restauración de copias de seguridad. -Instalar versiones actualizadas de software.
Uso inapropiado de recursos	Un incidente que involucra a una persona que viola alguna política de uso de recursos.	- Abuso de privilegios o de políticas de seguridad. Fuga de Información. - Mal uso y abuso de los servicios tecnológicos (correo, internet, intranet). - Captura de información confidencial. - Infracciones de derecho de autor y piratería. - Destrucción o alteración física de los componentes de red. - Destrucción o alteración de la información de configuración. - Uso prohibido del recurso de red.	**Contención** -Identificación del atacante. -Bloquear el usuario. -Aislarlo del recurso tecnológico. **Erradicación** -Restauración de copias de Seguridad. -Reconfigurar la seguridad de la base de datos. -Fortalecer y divulgar las políticas de seguridad. **Recuperación** -Restaurar los servicios o los componentes de red.

		- Uso indebido de información crítica. - Robo o pérdida de información. - Robo o pérdida de equipos.	
Código Malicioso	Programa o parte de éste insertado en otro con la intención de modificar su comportamiento original, usualmente para realizar actividades maliciosas como robo de información y de identidad, alteración o destrucción de la información y los recursos.	- Virus Informático. - Ransonware. - Malware.	**Contención** -Aislar equipo de la red. **Erradicación** -Corrección de efectos producidos. üRemover código malicioso. -Limpiar/Wiping/Zeroing. -Localizar la copia de seguridad limpia más reciente antes del incidente. -Mejora de las defensas. -Análisis de Vulnerabilidades. -Instalación de parches. **Recuperación** -Restauración de backups.
Reconocimiento	Se emplea para designar la acción de analizar, por medio de un programa, el estado de los puertos de una máquina conectada a través de una red de comunicaciones. Detecta si un puerto está abierto, cerrado o protegido por un cortafuegos o firewall. Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.	- Escaneo de puertos. - Intento de conexiones arbitrarias a través de un puerto.	**Contención** -Identificación y cierre de puertos. **Erradicación** -Incorporación de reglas de filtrado en el firewall. **Recuperación**
Vandalismo	Deformación o cambio producido de manera intencionada a la página web. Ataque al sitio web que cambia la apariencia visual del sitio. Los defacementingresan al servidor web y reemplazan el sitio web alojado por uno propio.	- Ataque por Injection de scripts Maliciosos. - Modificación del sitio web.	**Contención** -Suspensión del servicio web. **Erradicación** -Aplicar parches de seguridad faltantes. -Reparar el sitio web. **Recuperación** -Restaurar el servicio web.
			Contención -Uso de extintores. -Llamada a los bomberos si es el caso.

Daños Físicos	Son los sucesos del entorno y la naturaleza que causan daños a los activos de información, pueden ser causados por el hombre, la naturaleza o por averías del hardware y la infraestructura.	- Fuego. - Inundaciones. - Daños de hardware por fallos en el suministro de energía eléctrica. Terremotos y eventos naturales.	-Desconectar y retirar equipos
			Erradicación
			-Restaurar copias de seguridad. -Mantenimiento técnico de equipos para su recuperación. -Datacenter alterno. -Activación del plan de continuidad del negocio.
			Recuperación
			-Reinstalar equipos y dejar en funcionamiento.

4. Las actividades Post-Incidente se basan en el reporte apropiado del incidente, la generación de lecciones aprendidas, el establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

Lecciones aprendidas: Seguido a un incidente grave, y periódicamente después de los incidentes menores, se requiere la mejora de las medidas de seguridad y el proceso de gestión de incidentes, por lo tanto, es útil mantener un adecuado registro de lecciones aprendidas que permitan conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Evaluar si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas que puedan prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

3.7 Política de Seguridad Física y del Entorno

El centro de datos principal y otros cuartos en centros operativos donde se ubiquen equipos de comunicación o servidores, deben ser consideradas áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con las políticas de seguridad física.

3.7.1 Estándares para la Seguridad Física y del Entorno

Controles de acceso físico:

El acceso a las áreas clasificadas como restringidas en el área de TI centros de datos será monitoreado por personal del área de TI y estará limitado a:

- Desarrollo de operaciones tecnológicas.
- Pruebas de equipos.
- Mantenimiento de equipos y cableado estructurado.
- Arreglos locativos.

En los centros donde se encuentran servidores de datos se cuenta con un control de acceso biométrico administrado por el área de TI. En los otros casos, el acceso al centro de datos es autorizado por el Gerente del Centro Operativo en coordinación con el área de TI.

Uso del Centro de Datos:

El espacio destinado como centro de datos no podrá ser utilizado para almacenar elementos diferentes a los instalados por el área de TI, ni para desarrollar actividades distintas a las establecidas en los controles de acceso físico.

Seguridad de los equipos:

Los equipos deben estar conectados en todas las sedes a los circuitos de energía regulada (toma corrientes naranja e identificados generalmente con las iniciales CR), esto para prevenir la pérdida de información o daño en los activos de información y la interrupción de las actividades.

3.8 Política de Control de Acceso a la Información

El área de TI debe implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento.

3.8.1 Estándares para el Control de Acceso a la Información

Accesos privilegiados:

La asignación de usuarios especiales o privilegiados (como cuentas administrativas y supervisores) debe ser revisada cada 6 meses. Los administradores de la información son responsables de revisar los privilegios de los sistemas periódicamente y de retirar todos aquellos que ya no sean requeridos por los usuarios.

Servidores de aplicaciones y bases de datos, y otros dispositivos (excepto las estaciones de trabajo individuales) que son utilizadas para mantener funciones críticas del negocio, deben estar en un área de acceso restringido y separadas del ambiente de las oficinas.

Para el acceso a infraestructura crítica de la compañía debe ser únicamente para personal autorizado.

Para la revocación de permisos y eliminación de cuentas. Al finalizar la relación contractual con el empleado es necesario revocar sus permisos de accesos a nuestros sistemas e instalaciones. Se inactivarán sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, exigiremos la devolución de cualquier activo de información que se le hubiese asignado (tarjetas de acceso, equipos, dispositivos de almacenamiento, tokens criptográficos, etc.).

Registro de usuarios:

Cada usuario tiene una identificación única dentro de los sistemas de información. El usuario debe tener autorización de su jefatura inmediata para uso de los sistemas y servicios de la plataforma tecnológica. El nivel de acceso otorgado será el perfil definido de acuerdo con el cargo y funciones desarrolladas por el usuario.

Responsabilidades del usuario:

Los usuarios deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en especial lo que tiene que ver con el uso de contraseñas. El área de TI implementará los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, los colaboradores, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas, estas son personales e intransferibles.

Bloqueo de cuentas por inactividad:

Los sistemas de información funcionales dentro de la compañía contienen usuarios registrados con diferentes roles de acceso, los cuales pueden llegar a tener un tiempo de inactividad dentro de los sistemas de información debido a un periodo de vacaciones, incapacidades o retiro definitivo de la compañía. Por ello, los sistemas de información deben contar con la configuración junto a la ayuda del administrador y reporte entregado por el área de Gestión Humana para poder bloquear o dar de baja las cuentas de usuario(s) que se encuentren inactivas por un período de 60 días calendario.

En las cuentas de correo electrónico corporativo, se debe contar con el seguimiento del administrador y el reporte entregado por el área de Gestión Humana con el fin de bloquear o dar de baja las cuentas de correo electrónico de usuario(s) que se encuentren inactivas por un período de 60 días calendario.

Teniendo en cuenta lo anterior, para la reactivación de las cuentas dentro de los sistemas de información y correo electrónico corporativo se debe tener en cuenta lo siguiente:

Para la reactivación derivada de una ausencia por vacaciones, licencias o no uso de las cuentas, se requiere que el jefe inmediato apruebe a través de un requerimiento en la herramienta SysAid la reactivación de la cuenta de usuario en los sistemas de información o en la cuenta de correo electrónico corporativo. Si el jefe se encuentra ausente y se requiere autorización inmediata a la solicitud, esta podrá

realizarse con la aprobación del jefe de Gestión Humana.

La autorización será revisada y se dará respuesta dejando trazabilidad de la actividad dentro de la plataforma SysAid.

Si en algún momento se requiere la inactivación de alguna cuenta de acceso a los Sistemas de Información y/o cuenta de correo electrónico corporativo, debe ser con aprobación del nivel adecuado.

3.9 Política de uso y creación de contraseñas

Las contraseñas permiten la autenticación en los equipos de cómputo, sistemas de información y/o aplicaciones de la compañía. Las contraseñas siguen siendo a pesar de muchos esfuerzos por protegerlas, un eslabón débil dentro de la seguridad. La calidad de esta debe ser un factor importante para considerar. Las contraseñas son de uso personal e individual, no debe ser compartida con otras personas y debe ser mantenida en forma segura ya que si es descifrada puede traer problemas a la compañía.

3.9.1 Estándares para el uso y creación de contraseñas

- La longitud de la contraseña debe ser igual o superior a 8 caracteres.

- Utilizar en la misma contraseña números, letras mayúsculas, letras minúsculas y caracteres especiales o símbolos.

- Alternar las letras mayúsculas y letras minúsculas dentro de la contraseña.

- Utilizar caracteres especiales o símbolos tales como: ! " # $ % & ' ( ) * + , - . / : ;< = > ? @ [\ ] ^ _ ` { | } ~

- No se permite el uso de contraseñas que incorporen palabras en otro idioma, series consecutivas de números, cadenas con caracteres sucesivos del mismo dominio o la inclusión de información personal. Cualquier contraseña que no cumpla con las características de construcción mencionadas se definen como “contraseñas débiles”.

- La comunicación de la contraseña se realizará de forma secreta y personal vía el administrador y sin intermediarios, así mismo la cuenta entregada al usuario es intransferible y todas las acciones realizadas con ella quedan bajo la responsabilidad de este.

- En la primera autenticación del usuario se deben cambiar las contraseñas otorgadas por el personal del área de TIC por defecto en los sistemas de información y/o aplicaciones de **Alcanos de Colombia S.A. E.S.P.**

- El usuario tendrá derecho a cambiar su contraseña siempre y cuando cumpla con las características indicadas.

- Se tiene configurado un histórico de 10 contraseñas para que un usuario no pueda volver a usar una contraseña hasta que caduque el historial establecido.

- Por seguridad una cuenta de usuario se bloqueará después de 5 intentos fallidos, y solo podrá ser desbloqueada por el Administrador.

- La contraseña tendrá una caducidad de 60 días y el número mínimo de días entre los cambios de contraseña será de un día.

Acciones que deben evitarse en la creación de contraseñas seguras:

- No repetir los mismos caracteres en la misma contraseña. Ej: “000999”.

- Evitar usar cadenas de caracteres de sólo números, letras mayúsculas o minúsculas en la contraseña.

- No usar como contraseña, ni contener el mismo nombre de usuario asociado a la cuenta de acceso.

- No escribir la contraseña en un papel o documento donde quede evidencia de esta. Tampoco guardarla en documentos o notas rápidas dentro del propio computador o dispositivo móvil.

- No transmitir la contraseña por medio de correo electrónico, mensajes de texto o mensajería instantánea. Ni tampoco mencionarla verbalmente en una conversación personal o vía telefónica.

- Los sistemas de información deberán bloquear permanentemente al usuario luego de 3 a 5 intentos fallidos de autenticación.

- El usuario es autónomo de cambiar su contraseña en cualquier momento, pero en caso de que se haya presentado la más mínima posibilidad de que la misma haya sido comprometida, es necesario notificar a los administradores para efectuar el cambio urgente.

- No reutilizar contraseñas anteriormente usadas.

- No compartir la contraseña con otras personas y memorícela.

Excepciones

Cualquier excepción que se indica en la política para los sistemas de información estarán sujetas a la posible configuración adecuada.

3.10 Política de Gestión de Comunicaciones y Operaciones

El área de TI debe garantizar el funcionamiento correcto y seguro de la infraestructura tecnológica.

3.10.1 Estándares para la Gestión de Comunicaciones y Operaciones

Procedimientos y Responsabilidades

El área de TI debe definir controles que garanticen la apropiada operación tecnológica basados en los siguientes procedimientos:

- Copias de seguridad.

- Verificación de copias de seguridad.

- Radicación y atención de requerimientos al área de TI.

- Atención de requerimientos de desarrollo.

- Administración y control de acceso a usuarios.

Segregación de funciones

Las tareas y responsabilidades propias de gestión de tecnología y que están a cargo de funcionarios del área de TI, se deben segregar para reducir o impedir las oportunidades de acceso no autorizado a la red y cualquier modificación o mal uso de los activos de los sistemas de información. Se prestará especial cuidado a que una persona no pueda por si misma acceder, modificar o utilizar los activos, sin previa autorización y trazabilidad de las tareas realizadas.

Separación de ambientes

Los ambientes de desarrollo y pruebas y producción deben estar separados para reducir los riesgos de acceso o cambios no autorizados, prevenir fallos e implementar controles.

Administración de software

El área de TI es la única unidad autorizada para realizar cualquier modificación o instalación de *software* en los equipos de cómputo de la Compañía. El uso de software sin su respectiva licencia y autorización del área de TI, obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la Compañía, por lo que esta práctica no está autorizada.

El software instalado en los equipos es de propiedad de **Alcanos de Colombia S.A. E.S.P.**, la copia no autorizada de programas o de su documentación, su modificación, transformación, adaptación, des compilación o ingeniería inversa implica una violación a la política. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por **Alcanos de Colombia S.A. E.S.P.** o las sanciones que especifique la ley.

Copias de seguridad

Para garantizar la integridad y disponibilidad de la información y del código fuente de los sistemas de información de la Compañía, el área de TI administrará y ejecutará un sistema de copias de seguridad conservando los niveles de confidencialidad requeridos y verificando regularmente su efectividad. El sistema de copias de seguridad incluye un resguardo externo fuera de la sede principal de la Compañía.

Dispositivos de almacenamiento

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) puede ocasionalmente generar riesgos para la entidad al ser conectados a los equipos de cómputo, ya que son susceptibles de transmisión de virus informáticos o puede ser utilizado para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo, cuando estos han sido bloqueados por el área de TI, se debe obtener aprobación formal e individual del Área de TI a través de un requerimiento en la mesa de ayuda.

Gestión de seguridad en las redes

La conexión remota a la red de área local de la Compañía debe realizarse a través de una conexión VPN segura suministrada por el área de TI, la cual estará aprobada por el jefe inmediato de quien haga uso de la conexión o esté a cargo del contrato suscrito con el tercero. El acceso a la información de manera remota debe hacerse a los colaboradores y/o terceros de **Alcanos de Colombia S.A. E.S.P.**

Los dispositivos de cómputo externos a la infraestructura de red de la compañía deben cumplir con los siguientes requisitos mínimos de seguridad, evitando el ingreso de virus y programas maliciosos que lleguen a poner en riesgo la seguridad y operatividad de la infraestructura de red de la compañía:

- Todo equipo de cómputo externo que solicite la conexión inalámbrica a la red corporativa de la Compañía será evaluado por el área de TI para verificar que el equipo cuenta con las condiciones necesarias para darle ingreso a la red, se debe tener en cuenta que el área de TI tiene la autoridad para negar el ingreso de cualquier equipo que no cumpla con los requisitos mínimos de seguridad los cuales son: contar con un antivirus actualizado y una vez realizado el análisis no presentar infección por virus ni tener instalados programas maliciosos que puedan afectar la red.

- Una vez permitido el acceso del equipo de cómputo por parte del área de TI a la red corporativa, éste podrá ser monitoreado para verificar la trazabilidad en el caso de que se presente alguna eventualidad que afecte la seguridad de la red.

3.11 Política para Adquisición, Mantenimiento y Desarrollo de Sistemas de Información

El área de TI estará a cargo de gestionar y proveer las medidas de seguridad en sistemas de información en su proceso de desarrollo para nuevas aplicaciones o de mantenimiento para las existentes.

3.11.1 Estándares para la adquisición, mantenimiento y desarrollo de sistemas de información

Requerimientos de seguridad de los sistemas.

El área de TI debe asegurar que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información consideren la administración de los riesgos de seguridad, reflejados en el establecimiento de los controles correspondientes.

La adquisición de todo aplicativo informático o software debe contar con la aprobación del área de TI en lo relacionado con el cumplimiento de los requerimientos de seguridad establecidos en esta política.

Seguridad de las aplicaciones del sistema.

El desarrollo interno y por contratación de aplicaciones debe cumplir con requerimientos mínimos de seguridad, conforme a las buenas prácticas en seguridad de la información y a esta política de seguridad. El diseño y operación de los sistemas debe obedecer a estándares de seguridad comúnmente aceptados y la normatividad vigente.

Seguridad de los sistemas de archivos.

Se debe controlar el acceso al código fuente de las aplicaciones y su sistema de archivos de parametrización.

Seguridad de los procesos de desarrollo y soporte.

Los procesos de desarrollo y soporte deben garantizar que el personal a cargo de estas tareas cuente con los privilegios exclusivos para esto, cumplan con los niveles de autorización y aprobaciones establecidos y actualicen la documentación correspondiente.

3.12 Política para el Cumplimiento con la Legislación Vigente

Toda solución de servicios o infraestructura tecnológica debe garantizar que está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de la regulación que afecta a la compañía.

3.12.1 Estándares para el Cumplimiento con la Legislación Vigente

Propiedad intelectual.

Se protegerá la propiedad intelectual de **Alcanos de Colombia S.A. E.S.P.** (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

Protección de datos.

Los estándares de seguridad son de obligatorio cumplimiento para los colaboradores o terceros con acceso a datos de carácter personal y a los sistemas de información. Deberán considerar, los siguientes aspectos:

- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley.

- Funciones y obligaciones del personal con acceso a las bases de datos.

- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.

- Procedimientos de realización de copias de respaldo y de recuperación de los datos.

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	ELABORÓ
4	05/Feb/2021	SE REALIZA ELABORACIÓN DE PLANTILLA DEA-05-001 DEBIDO A QUE EL DOCUMENTO SE ENCONTRABA EN PLANTILLA INST-05-006 Y NO CUMPLIA CON LA ESTRUCTURA JERARQUICA DOCUMENTAL. INCLUSIÓN DEL APARTADO 3.6 RELACIONADO CON LAS DIRECTRICES Y GESTIÓN A SEGUIR PARA EL REPORTE DE INCIDENTES DE SEGURIDAD	M.C. LEYTON

ELABORÓ	Vo Bo /REVISÓ	APROBÓ
Nombre: Nayla Vanessa Valenzuela Munoz **Cargo:** Analista Calidad **Fecha:** 05/Feb/2021	**Nombre:** Alvaro Francisco Nieva Pinilla **Cargo:** Jefe de HSEQ **Fecha:** 05/Feb/2021 **Nombre:** Maria Catalina Leyton Torres **Cargo:** Jefe de Sistemas **Fecha:** 05/Feb/2021	**Nombre:** William Fernando Oviedo Rojas **Cargo:** GERENTE GENERAL **Fecha:** 05/Feb/2021