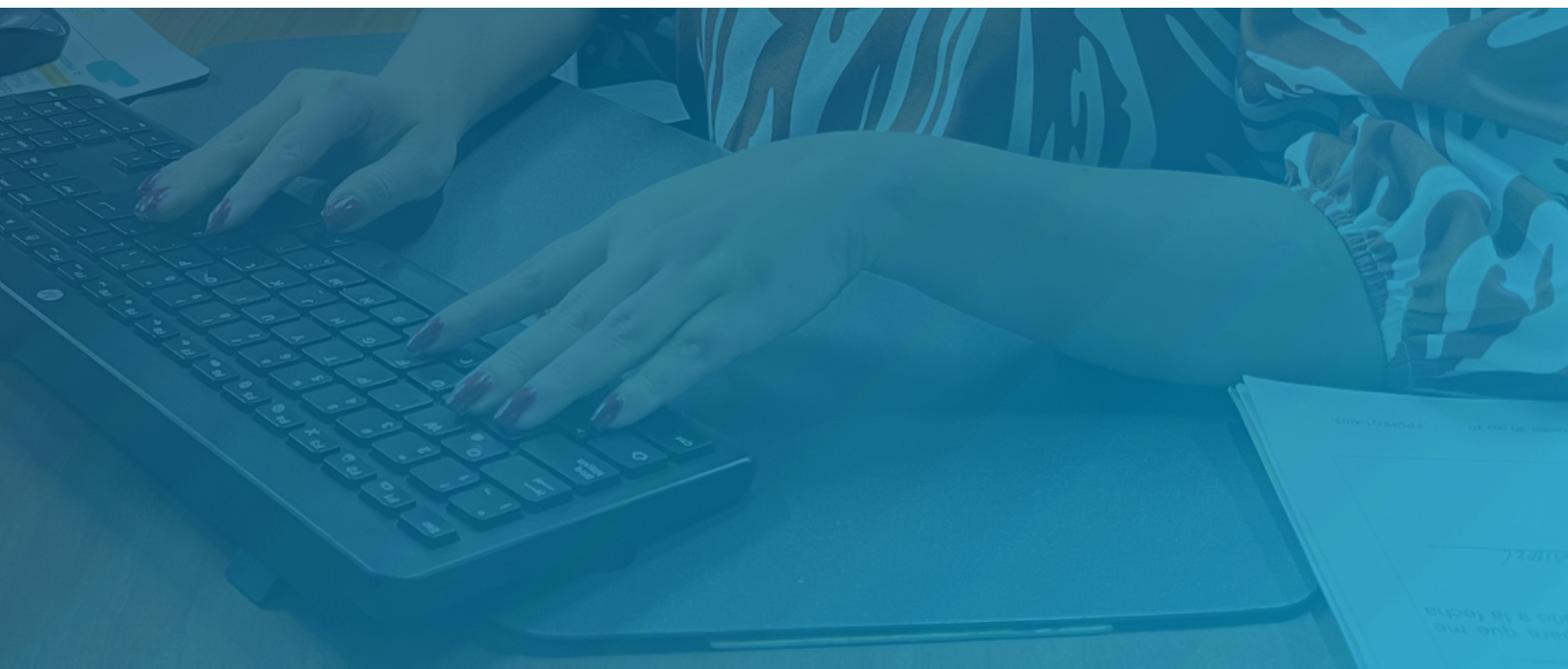
SuperPack

Política de Seguridad de la Información



Política de Seguridad de la Información

SuperPack

Contamos con un conjunto de reglas, prácticas y procedimientos diseñados para **proteger la confidencialidad, integridad y disponibilidad de nuestra información.**

Nuestro objetivo es claro: **establecer directrices que garanticen la protección de datos sensibles y críticos,** minimizando riesgos frente a amenazas como accesos no autorizados, pérdida de datos y otros incidentes de seguridad. **Todos somos responsables de manejar la información con cuidado y compromiso.**

Puedes acceder al contenido completo de nuestra **Política de Seguridad de la Información** en cualquier momento a través de nuestro sitio web: **www.superpack.com.co** o en el **documento de políticas** entregado al momento de unirte a SuperPack.

¿Qué es?

Una política de seguridad de la información es un conjunto de reglas, prácticas y procedimientos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Estas políticas son esenciales para garantizar que la información crítica se maneje de manera segura y se proteja contra amenazas como accesos no autorizados, pérdida de datos, y otros riesgos de seguridad.

1. Objetivo:

Establecer un marco y un conjunto de directrices que guíen a la compañía en la protección de la información sensible y crítica. Esta política es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para mitigar los riesgos asociados con posibles amenazas y vulnerabilidades.

2. Alcance:

La política de seguridad de la información debe impactar y ser aplicable a toda la compañía y todos los niveles jerárquicos tales como gerencia, gestión humana, personal de TI, usuarios finales de las distintas áreas del proceso productivo, socios, proveedores y clientes.

3. Desarrollo

3.1 Condiciones Generales

3.2 Socialización y entendimiento por parte de todos los funcionarios de la compañía sobre la importancia de la política de seguridad de la información, la necesidad de aplicarla, los riesgos a los que se exponen los datos como el activo más importante de la organización y que ocurriría si no se cumple a cabalidad con estos lineamientos. La difusión de la política será con el apoyo del área de comunicaciones, quienes con correos oficiales y piezas publicitarias informaran sobre las buenas prácticas y el adecuado uso de las herramientas tecnológicas entregadas tanto de software como hardware y la aceptación de la responsabilidad sobre las mismas.

3.3 Definir y dar el rol de administrador sobre las herramientas tecnológicas al área de TI para ser el regulador de las políticas requeridas tales como, asignación de equipos, creación de usuarios de dominio con sus roles definidos, gestión y control de accesos, creación de parámetros de contraseña segura, uso de pendrive, niveles de protección vía antivirus en los cuales se establecerán restricción a sitios y páginas, permisos definidos en accesos a aplicativos implementados por la compañía para desarrollar las tareas de cada una de las áreas, control y seguimiento en la tenencia de los equipos de cómputo.

3.4 Creación de usuario en el Active Directory: Este deberá ser solicitado por medio de una PQR al área de TI y debe contar con el Formulario Solicitud de creación o modificación de usuarios. El proceso que se describe a continuación es la forma en la que se deberá crear el usuario y su perfil.

3.5 Parámetros de Contraseña Segura: Una contraseña segura no se puede determinar fácilmente adivinándola o utilizando programas automáticos, son la primera línea de defensa contra los ciberataques y pueden reducir el riesgo de una vulneración de seguridad de la información o los dispositivos. La creación de la primera contraseña será por parte del equipo de TI, el usuario deberá cambiarla en su primer uso con las especificaciones detalladas en la imagen, se renovará necesariamente cada 60 días y será avisado por medio de anuncio en su computador, es de uso personal, no deberá compartirse con ningún otro usuario. Esta norma es de estricto cumplimiento para todos los empleados de la compañía y el área encargada de su regulación y supervisión es el equipo de TI.

3.6 Uso de pendrive, niveles de protección vía antivirus, restricción de sitios:

3.6.1 Es importante establecer políticas claras sobre el uso de pendrive en entornos corporativos, limitar su uso solo a equipos autorizados, evitar conectar pendrives desconocidos, y generar conciencia en los usuarios ya que este puede representar un riesgo de seguridad, contener malware o ser utilizados para la exfiltración de datos de manera no autorizada. Esta norma es de estricto cumplimiento para todos los empleados de la compañía y el área encargada de su regulación y supervisión es el equipo de TI. **Ver Manual de ONDRIVE**

3.6.2 Los programas antivirus son herramientas fundamentales para proteger los sistemas contra virus, malware, ransomware y otras amenazas cibernéticas. El equipo de TI debe mantener el software antivirus licenciado, actualizado, de buena reputación, realizar análisis periódicos, detección en tiempo real, capacidad de bloqueos conocidos y desconocidos, generar niveles de seguridad para los diferentes grupos de usuarios de la compañía.

3.6.3 La restricción de sitios web o el filtrado web se realiza por medio del endpoint, es útil para controlar el acceso a contenido no deseado o potencialmente peligroso, como sitios maliciosos, de phishing o con contenido inapropiado. El equipo de TI deberá tener configuración de políticas de seguridad en los navegadores web, el uso de firewalls de red, filtrado de contenido y generar un equilibrio adecuado entre las políticas de seguridad aplicadas en la red y el uso de estas para los usuarios, de modo que no se genere una excesiva restricción que pueda afectar la productividad de los empleados.

Se posee 3 niveles de Acceso Básico que es el que es el general para todos los empleados de la empresa, y sobre se crean las excepciones a nivel de páginas requeridas para los diferentes puestos de la empresa; Acceso Medio este es para aquellas personas que requiere categorías de paginas mas avanzadas como son de páginas de contenido de videos, redes sociales, ETC; y el Acceso avanzados es para aquellas personas Directivos y personal de TI.

3.7 Uso del Correo Electrónico: Todos los mensajes generados a través de la plataforma de correo electrónico office365 de Superpack se consideran propiedad de la compañía, está restringido a correos oficiales y no debe usarse para asuntos personales.

Está prohibido utilizar el sistema de correo para el desarrollo de actividades políticas, comerciales o de entretenimiento o para la transmisión de mensajes vulgares u obscenos, por seguridad no se debe dar la clave para acceder al servicio a terceras personas. No se debe utilizar el correo electrónico para participar en la propagación de cartas en cadena o participar en esquemas piramidales o temas similares. El manejo de las claves de seguridad y la información que se tramita en cada cuenta es responsabilidad única del funcionario.

3.8 Software en los Computadores: Todo software que se utilice en los equipos de Superpack será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la entidad o reglamentos internos, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual. El usuario no puede instalar ningún programa ya que es el área de TI quienes tienen los permisos de administrador sobre los equipos. La instalación de software que desde el concepto técnico del área de sistemas ponga en riesgo los recursos de la institución no está permitida.

3.9 Almacenamiento de archivos dentro de la Red: La información personal como fotos, archivos, publicaciones y demás, no deben ser guardados en carpetas, OneDrive o NAS de la compañía. Los usuarios de la infraestructura tecnológica de Superpack no pueden dañar o borrar el trabajo de otros funcionarios. El uso indebido o deliberado de los archivos de la red y de su equipo se considerará como un acto de vandalismo y podrá ser causa de una acción disciplinaria.

Todos los archivos de índole corporativo para para uso personal debe de estar contenido en el OneDrive de cada personal y todos aquellos archivos que se van a trabar de manera colaborativa o que van a ser trabajada por 2 más o personal de la organización se deben de compartir desde SharePoint.

3.10 Uso de Internet: El usuario no debe entrar a páginas web con contenido pornográfico o inapropiado, tampoco podrá bajar ningún software sin la debida autorización del área de tecnología; el usuario no puede utilizar redes sociales salvo sean autorizados y no se debe utilizar el internet con fines comerciales, políticos o con propósitos ilegales.

Está prohibido el uso de acceso a internet para acceder, crear, copiar, distribuir material o enviar mensajes obscenos, pornográficos, etc., o mensajes que inciten a violencia o amenaza de cualquier tipo.

Los usuarios que tienen acceso a Internet a través de la red de Superpack deberán aceptar, respetar y aplicar las políticas y prácticas de su uso ya que se realizaran constantes auditorías con el fin de verificar el buen uso del recurso y al ser encontrado algún usuario dando un indebido uso a esta herramienta, se procederá a comunicarle al jefe de área, sobre los hallazgos encontrados.

3.11 Seguridad de la Información: Los usuarios de la infraestructura tecnológica de Superpack deberán garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma y esto se realizara con el acompañamiento del área de TI quien desde la restricción de permisos complementara la acción. Se deberá garantizar la integridad y salvaguardar la exactitud y totalidad de la información y su autenticidad; se debe asegurarla validez de la información en tiempo, forma y distribución. Así mismo, se garantizará el origen de la información, validando el emisor para evitar suplantación de identidades. Sera necesario generar auditorias periódicas a fin de que todos los eventos que ocurran en el sistema puedan ser registrados para su control posterior.

3.12 Acceso por parte de Terceros: Cuando exista la necesidad de otorgar acceso a terceras partes a información de la compañía, el responsable del área de TI y el propietario de la Información, realizaran una evaluación de riesgos para identificar controles específicos; teniendo en cuenta aspectos como el tipo de acceso requerido ya sea físico o lógico y a qué recurso, los motivos para los cuales se solicita el acceso, el valor de la información, los controles empleados por el tercero y la incidencia de este acceso en la seguridad de la información de la compañía.

3.13 Tercerización en requerimientos de seguridad en Contratos: Los contratos o acuerdos de tercerización total o parcial para la administración, control de sistemas de información y la red de Superpack, contemplarán además del ítem 3.12 controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información, derecho a la auditoría por parte del área de TI y los contratos deben prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes involucradas.

3.14 Clasificación y Control de Activos: Superpack hará control de todos sus activos fijos con el propósito llevar un registro de todo el ciclo de vida de su inventario, se especificaran características como tipo de elemento, fecha de compra, cantidad, valor, depreciación, ubicación y estado de todos los elementos adquiridos para desarrollar las actividades propias del negocio; este será controlado a través de la ERP siesa y por su parte el área de TI también tendrá que llevar un control especifico de todo el parque informático que incluya software y hardware de la compañía por medio de su herramienta Helpdesk GLPI.

Este control por medio etiquetas tendrá un código único del activo y facilitará la identificación y seguimiento preciso del elemento, esto permitirá generar planes de acción en la renovación de licenciamientos, recambios por obsolescencia, daños, pérdida o robo, identificar y llevar historial de los eventos para planificar financieramente el gasto del área de TI.

3.15 Backups de información de usuarios, servidores, y bases de datos: Es de importancia de primer nivel para garantizar la seguridad y disponibilidad de los datos en caso de fallos, errores humanos, ataques cibernéticos u otros eventos adversos. Se definirá por parte del área de TI de Superpack una planificación de los respaldos que indicarán frecuencia, formato, sitio de almacenamiento, redundancia, protección de los datos, backups incrementales y completos que permitan salvaguardar la información como uno de los activos más importantes de la compañía.

Nota: A los equipos de usuarios finales no se realiza Backup de la información contenidos en ellos por eso se tiene como política Numeral 3.9 “Todos los archivos de índole corporativo para para uso personal debe de estar contenido en el OneDrive de cada personal y todos aquellos archivos que se van a trabar de manera colaborativa o que van a ser trabajada por 2 más o personal de la organización se deben de compartir desde SharePoint.”

3.16 Sanciones por incumplimiento de la política de seguridad: Es importante que la política de seguridad de la información sea difundida y conocida por todos los empleados de la compañía, ya que esto permitirá que se establezcan claramente los procedimientos permitidos en el uso de los recursos tecnológicos y los acuerdos en las posibles sanciones por incumplimiento, así como los procedimientos para aplicarlas de manera justa y consistente. Además, es fundamental que todos los empleados estén conscientes de estas políticas y de las consecuencias de no cumplirlas.

Algunas de estas sanciones podrán ser:

- **Amonestaciones:** En casos leves o cuando el incumplimiento es accidental, es posible que se emita una advertencia formal al empleado responsable.

- **Formación Adicional:** Si el incumplimiento se debió a la falta de comprensión de las políticas de seguridad, el área de TI podría requerir que el empleado reciba formación adicional sobre las políticas y procedimientos de seguridad.

- **Suspensión temporal o llamado de atención por escrito con copia al jefe de área:** En casos más graves, la empresa podría imponer un memorando escrito con copia a su jefe de área para que no sea repetitiva la falta o definir una suspensión temporal al empleado como medida disciplinaria.

- **Deducciones de Salario:** Dependiendo de la gravedad del incumplimiento y las políticas de la empresa, podría imponerse una deducción de salario al empleado responsable, sobre todo en la responsabilidad del activo fijo asignado como es el caso del computador. (acá se hará la investigación pertinente del evento ocurrido).

- **Acciones Disciplinarias:** En casos extremos de incumplimiento grave o repetido, la empresa podría tomar medidas disciplinarias más severas como la pérdida de privilegios y permisos en acceso a aplicativos o fuentes de información o incluso la terminación del contrato laboral.

- **Responsabilidad Legal:** En situaciones donde el incumplimiento de la política de seguridad resulta en daños significativos para la empresa o terceros, podría haber consecuencias legales, incluyendo demandas civiles o acciones penales, dependiendo de las leyes y regulación actual.

CLASIFICACIÓN DE LAS FALTAS

Política de Seguridad de la Información

SuperPack

FALTAS LEVES

Las faltas leves tienen consecuencias para la seguridad de la información y es fundamental que los usuarios protejan los activos de la organización garantizando la confidencialidad, integridad y disponibilidad de los datos.

- **Incumplimiento de procedimientos:** estos pueden incluir no cambiar regularmente las contraseñas con las indicaciones de TI o ausentarse del puesto de trabajo sin bloquear su equipo dejando expuesto su acceso a otros usuarios, no realizar copias de seguridad de los datos en OneDrive.

- **Acceso no autorizado:** Acceder a información o sistemas sin la debida autorización, incluso si no se produce un daño real.

- **Uso inadecuado de recursos:** Utilizar los recursos de TI de manera inapropiada, como instalar software no autorizado o visitar sitios web no relacionados con el trabajo durante horas laborales.

- **Falta de concienciación:** No participar en programas de formación o no estar al tanto de las políticas de seguridad.

- **Negligencia en la protección de datos:** No proteger adecuadamente los datos confidenciales o personales, como dejar documentos impresos en áreas públicas o no cifrar archivos sensibles.

- **No informar incidentes de seguridad:** No reportar incidentes de seguridad, como la pérdida de dispositivos, la detección de malware o apertura de correos sospechosos.

FALTAS GRAVES

Se estipula que una falta es grave cuando una falta leve se vuelve repetitiva o la infracción tiene una consecuencia significativa para la compañía o sus empleados.

- **Incumplimiento de procedimientos críticos:** No seguir los procedimientos establecidos en la PSI, o no proteger adecuadamente los datos confidenciales.
- **Acceso no autorizado a información sensible:** Acceder a datos o sistemas sin la debida autorización, especialmente si esto compromete la confidencialidad o integridad de la información.
- **No reportar incidentes de seguridad:** No informar de manera oportuna sobre incidentes de seguridad, lo que podría poner en riesgo la organización y su reputación.

- **Conducta fraudulenta o corrupta:** Participar en actividades fraudulentas, corruptas o deshonestas relacionadas con la seguridad de la información, utilización indebida de los recursos tecnológicos.
- **Revelación no autorizada de información confidencial:** Divulgar a terceros datos sensibles o secretos comerciales sin la debida autorización.
- **Conexiones no permitidas Remotas:** Solo el personal de TI o a quienes esta área autorice de empresa para realizar conexiones autorizados para realizar conexiones remotas a los equipos o servidores, en caso de que un tercero requiera conexión debe de ser coordinada con el área de TI para validar los motivos y realizar el acompañamiento.
- **Sincronización de OneDrive:** Solo esta autorizado en equipos de la empresa.

FALTAS MUY GRAVES

Es considerada una falta muy grave aquella que trae consecuencias trascendentales para la organización y sus empleados, incluso que acarree sanciones de tipo económico o legal.

- **Incumplimiento del secreto profesional:** Revelar información confidencial o sensible sin la debida autorización es una falta muy grave. El secreto profesional es fundamental para proteger la privacidad de los datos y la integridad de la información.

- **Brechas de seguridad:** Accesos no autorizados a sistemas informáticos o redes, lo que puede resultar en robo, divulgación o alteración de información confidencial.

- **Phishing e ingeniería social:** Participar en actividades fraudulentas diseñadas para engañar a los compañeros y obtener información confidencial, como contraseñas o información a través de correos electrónicos falsos o spam.

- **Sabotaje o daño intencional:** Realizar acciones deliberadas para dañar sistemas, redes o datos, ya sea por venganza o con fines maliciosos.

- **Manipulación maliciosa de datos:** Alterar intencionalmente datos o registros para beneficio personal o para dañar a la organización.

4. REVISIÓN DEL DOCUMENTO:

Este documento se revisa en dos años a partir de la fecha de aprobación, o si se presenta alguna modificación antes de esta fecha, se procede a su revisión inmediatamente.

5. EVALUACIÓN:

Después de haber realizado la divulgación y publicación en nuestro sistema de gestión documental, los colaboradores de SUPERPACK. S.A.S quedan certificados y se entiende que conocen la política de seguridad de la información de la compañía.

PTIC001(01)
Fecha de creación: 20-04-2024.
Fecha de aprobación: 23-05-2024.
Elaborado por: Coordinador de TIC – Bibiana Betancur.
Revisado y Aprobado por: Jefe de TIC – Jaime García.