Palmicultores del Norte S.A.S., se compromete con el manejo de la seguridad informática, definiendo, formulando, promoviendo, políticas y estrategias para la protección electrónica de la información de la empresa aportándole confidencialidad, integridad y disponibilidad de esta.

Los datos personales que se recolectan cumplen con su objeto social y las obligaciones legales asociadas. Para garantizar el adecuado manejo de esta información, se ha implementado la política **LEG-01-PL-10** tratamiento de datos personales, la cual establece los procedimientos y canales específicos para el tratamiento de datos personales sensibles y generales. Esta política asegura el cumplimiento legal al artículo 15 y 20 de la Constitución Nacional, la Ley 1581 de 2012, el Capítulo 25 del Decreto 1074 de 2015 y la Sentencia C-748 de 2011. las normativas de protección de datos y está dirigida a todos los titulares de la información, incluyendo empleados, clientes, proveedores, accionistas y cualquier otra persona cuyos datos personales sean tratados por la organización.

La política **LEG-01-PL-10** contempla los principios de confidencialidad, seguridad y acceso restringido, permitiendo a los titulares de los datos conocer cómo se manejará su información y asegurando su protección frente a accesos no autorizados. Además, define los medios de recolección, almacenamiento y uso de los datos, respetando los derechos de los titulares y las disposiciones de la ley aplicable.

Criterios Generales

Podrá expedirse autorización de acceso a la plataforma de tecnologías y sistemas de información a empleados, proveedores de servicios y/o estudiantes, que por la naturaleza de sus actividades requieran acceder a estos servicios en forma permanente o periódica durante el ejercicio de sus actividades, previa solicitud al jefe de sistemas, realizada por el coordinador responsable de las actividades.

La información generada por los empleados, contratistas, estudiantes en desarrollo de las actividades propias de la empresa es propiedad de PALNORTE S.A.S., a menos que se acuerde lo contrario en los contratos escritos y autorizaciones de los propietarios de los datos.

Los programas que se manejen o sean diseñados por la empresa y sean suministrado por proveedores, estos deberán tener un documento firmado de derechos de autor a nombre de PALNORTE S.A.S.

Política de seguridad informática

PALNORTE S.A.S. cuenta con una política de seguridad informática aprobada por la gerencia, actualizada, publicada en su sitio web y que debe ser difundida a todo el personal de la empresa. De igual manera debe ser revisada periódicamente para asegurar su conveniencia, adecuación y eficacia.

Roles y Responsabilidades

Usar bien la información que resulta de las actividades desarrolladas en PALNORTE S.A.S.

Es competencia del área de Tics de la entidad la definición de los roles, responsabilidades y competencias en seguridad de la información.

En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.

Todos los empleados y terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos y aquellas que la modifiquen o sustituyan, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información del Ministerio.

Gestión de Talento Humano

Al ingreso de empleados, contratistas, estudiantes, que requieran hacer uso de los activos de la información, deberán conocer y apropiar el presente manual.

En la descripción de las responsabilidades de los puestos de trabajo se incorporarán las funciones y responsabilidades de seguridad. De igual manera, se firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información. La copia de este compromiso se archivará seguramente en las historias laborales de cada empleado o en la carpeta contractual o del convenio para proveedores y estudiantes.

Al momento de la terminación de contrato o finalización de labores de un empleado, contratista o estudiante, debe ser informado por la oficina de Talento Humano a Tics para proceder a la inactivación de los usuarios y para que sean eliminados los accesos a la red y sistemas de información que tenga asociados.

Se debe resguardar la reserva de los documentos y bases de datos que contengan información personal de funcionarios y terceros que laboran o laboraron en la entidad.

Se debe capacitar a todos los empleados, contratistas, estudiantes y solicitantes de accesos a activos de información sobre el uso y la responsabilidad que tienen al ser autorizados.

Selección de personal:

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación.

Se deben aplicar los controles establecidos por la empresa para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la Entidad.

El área de Talento humano y Contratación son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales; los cuales deben ser anexados a la documentación requerida para la contratación.

Procesos disciplinarios:

Todos los incidentes de seguridad de la información presentados en PALNORTE S.A.S. deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

En lo pertinente a la violación de las políticas de seguridad de la información de la Entidad, a los empleados y terceros, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

Gestión de activos

Los activos de información pertenecen a la empresa y el uso de estos debe emplearse exclusivamente con propósitos laborales. Se prohíbe el borrado de información que pertenece a la empresa, así como su manipulación con fines diferentes a los laborales.

Todos los activos de información deben tener un propietario, custodio y deben estar debidamente identificados.

La Entidad asignará dispositivos móviles (computadores portátiles, celulares, tabletas) a empleados y contratistas, de acuerdo con la disponibilidad de equipos y servicios, así como la función a desempeñar, previa solicitud al jefe de Tics.

Los activos de información se clasifican según la criticidad, sensibilidad y reserva de esta. Se realiza etiquetado de la información identificando el responsable de este.

Solo los funcionarios del área de Tics están autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la entidad, así como herramientas para hacer tareas de mantenimiento, revisión de software, recuperar datos perdidos y eliminar software malicioso.

Se prohíbe el uso del almacenamiento de archivos Online, es decir, en aquellas unidades virtuales de almacenamiento personal por medio de internet. Por lo que se prohíbe: Almacenar o transportar información clasificada o reservada, ejecutar cualquier tipo de programa no autorizado por la empresa desde cualquiera de las unidades de almacenamiento externo, descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en los equipos informáticos.

En caso de ser necesario y previa autorización de la Gerencia, los usuarios de la empresa podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.

Los usuarios deberán utilizar únicamente los programas y equipos autorizados por Tics.

Todas las aplicaciones deben contar con licencia, si llegase a vencer alguna se debe informar a Tics para su gestión.

Los recursos informáticos que tiene dispuesta la empresa no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales, por ejemplo: música, videos, películas o imágenes de índole personal.

Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, borrado de archivos, etc.

Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de Tics:

- Copiar o distribuir cualquier software de propiedad de la empresa.
- Cambiar la configuración de hardware de propiedad de la empresa.
- Hacer uso de la red de datos de la empresa para bajar o descargar software de Internet u otro servicio en línea en equipos diferentes a los de la empresa.
- Modificar, revisar, transformar o adaptar cualquier software propiedad de la empresa.
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la empresa.

Tics debe avisar previamente a través de la herramienta de mesa de ayuda en línea PALMIDESK, de cualquier traslado de recursos informáticos, para garantizarse su correcto funcionamiento posterior.

En el traslado de equipo o de información, se deben tomar precauciones para no borrar información sensible para la empresa; por eso se recomienda que los funcionarios de Tics estén bajo la supervisión.

La copia de seguridad de la información está bajo la responsabilidad de Tics, sin embargo, el usuario debe velar porque éste se realice periódicamente y a los archivos que corresponda.

Los equipos móviles que accederán a la red de datos de la empresa deberán autorizar el responsable de Tics.

Los funcionarios deberán devolver todos los activos físicos y/o electrónicos asignados por la empresa en el proceso de desvinculación, así deberán documentar y entregar a la empresa información y los conocimientos importantes de la labor que ejecutan consignándolo en un acta de entrega a su jefe para continuar con los trámites de finalización del empleo.

Control de Acceso

Para el control de acceso a los servicios de TI, la Entidad realizará las configuraciones de red, mediante la creación de usuarios, control de directivas de red, protocolo de control de acceso, certificados para la autenticación; definidos e implementados por la oficina Tics.

La entidad debe definir los servicios de TI a publicar en las redes internas y externas, para lo cual debe definir la segmentación de la red, perfiles de acceso para el acceso a los servicios que administra la oficina Tics.

La oficina Tics deberá generar la segmentación de redes y los perfiles de acceso, de acuerdo con la capacidad y disponibilidad de servicios de TI.

La oficina de Tics debe implementar y administrar una red inalámbrica con perfiles para acceso a los servicios red de la entidad.

La configuración de acceso a correo electrónico institucional en dispositivos móviles personales se realizará únicamente a usuarios de la Entidad, previa solicitud realizada a través de la herramienta de soporte de servicios en línea o mesa de ayuda por el usuario y debe contar con el visto bueno del Coordinador de la oficina TIC's.

Por el consumo de ancho de banda, se restringe el uso al personal no autorizado de programas o visores web como YOUTUBE, páginas de música y de descarga.

No se podrá ingresar a páginas de contenido para adultos (páginas pornográficas, películas, chats en vivo y demás).

Las páginas WEB que emita aviso de riesgo o peligro no tendrán autorización por la empresa para su ingreso.

Establecimiento, uso y protección de claves de acceso

Se debe concientizar y controlar a los usuarios para aplicar buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, que constituyen un medio para validar la identidad de un usuario y establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".

Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.

Ningún usuario deberá acceder a la red o a los servicios TIC de la entidad, utilizando una cuenta o clave de otro usuario.

Los usuarios deben tener en cuenta los siguientes aspectos:

- No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo, almacenadas en un macro o recordatorio en navegadores web.
- El cambio de contraseña solo podrá solicitarlo el titular de la cuenta, dirigiéndose a la oficina Tics, donde se validará los datos personales; si se solicita el cambio de contraseña para otra persona, debe realizarlo su jefe inmediato (previa autorización del Coordinador de la oficina Tics).
- Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
- Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por tres veces.
- La clave de acceso la desbloquearán solo funcionarios de la oficina TIC, tras la solicitud formal del responsable de la cuenta.
- Es responsabilidad del usuario el manejo apropiado a las claves asignadas de los servicios de red y de acceso a la red estas claves de acceso y usuarios son personales e intransferibles.
- Los usuarios y claves de los administradores de sistemas y del personal de la oficina TIC de la Información son de uso personal e intransferible.
- El personal de la oficina TIC debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo con el rol asignado.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Coordinador de la oficina TIC.

Las claves o contraseñas deben:

- Poseer algún grado de complejidad.
- No deben ser palabras comunes que se puedan encontrar en diccionarios.
- Ni tener información personal.
- Ni productos a resaltar de su entidad.
- Evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

- Los usuarios no deben usar sus contraseñas personales en el entorno laboral.
- La contraseña debe tener mínimo ocho caracteres alfanuméricos.
- La contraseña debe cambiarse la primera vez que el usuario ingrese al sistema.
- La contraseña debe cambiarse cada 60 días como mínimo, o cuando lo establezca la oficina Tics.
- Cada vez que se cambien las claves, estas deben ser distintas por lo menos de las últimas tres anteriores.
- Se debe cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- La contraseña, no se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- La clave de acceso no debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas.
- Caracteres en minúsculas.
- Base de 10 dígitos (0 a 9).
- Caracteres no alfabéticos (Ejemplo ¡,$, %, &).

Las contraseñas de acceso no deben ser reveladas a ninguna persona, incluyendo al personal de Tics.

No registrar las contraseñas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

Generación de cuentas de usuario

La generación de cuenta de usuario se realizará posterior a la aprobación de la solicitud realizada a través de la herramienta de soporte de servicios en línea o mesa de ayuda disponible en la intranet de la Entidad, acorde con el procedimiento creación, actualización y desactivación de usuarios.

En la solicitud de creación de cuenta, se debe indicar el acceso a aplicativos y el perfil de navegación de internet que requiere por su cargo y funciones a desempeñar.

Para el ajuste o modificación a los niveles de navegación o la aprobación de acceso a aplicativos, el jefe directo del usuario que lo requiere debe realizar una solicitud a través de la herramienta de soporte de servicios en línea disponible en la intranet de la Entidad con el visto bueno del jefe de Tics.

La oficina de TIC's en acompañamiento con los coordinadores de oficina deben realizar periódicamente revisión de los permisos de acceso de los colaboradores a cargo, así como de los que tengan acceso a su módulo de gestión.

Seguridad física y del entorno

El retiro e ingreso de todo activo de información de los visitantes que usen las instalaciones de PALNORTE S.A.S. (consultores, pasantes, visitantes, etc.) será registrado e inspeccionado en los controles de accesos a la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.

La Entidad destinará un área de acceso restringido, donde se ubicarán los servidores o almacenamiento de información, la infraestructura que soporta los sistemas de información y comunicaciones, por lo cual se deben emplear mecanismos de control de acceso físico que garanticen que sólo se permite el acceso al personal autorizado.

Las áreas de acceso restringido deben contar con condiciones ambientales adecuadas tanto de temperatura, humedad, polvo, especificados por los fabricantes de los equipos en funcionamiento, y contar además con las hojas de vida de cada equipo, con su historial de mantenimientos preventivos y correctivos.

El acceso a las áreas restringidas por parte del personal de soporte técnico de proveedores se debe solicitar por medio de una autorización con el visto bueno del jefe de la Oficina TIC's, con supervisión de un funcionario de la oficina de TIC´s.

Todos los proveedores y contratistas deben portar en un lugar visible el carnet que los identifica para el acceso a la empresa y mientras se encuentren dentro de ella.

Se debe avisar al responsable de TI para cualquier traslado de recursos informáticos, para garantizarse el correcto funcionamiento posterior de estos.

En el evento de un traslado de equipo o de información, se deben tomar las precauciones necesarias para no realizar borrado de información sensible para la empresa; por tal motivo se recomienda que siempre sea bajo la supervisión de la oficina de TIC's.

Se debe llevar un control de ingreso y salida del personal que visita el centro de datos, que debe diligenciarse al iniciar y finalizar la actividad.

Solo el responsable de Tics puede autorizar el ingreso de computadores, dispositivos de comunicación y herramientas destinadas a las labores específicas de trabajo en las áreas de procesamiento de datos.

El responsable de Tics debe autorizar expresamente la grabación de vídeo en las instalaciones del centro de datos o centrales de cableado con fines institucionales.

El responsable de Tics con el jefe de mantenimiento de PALNORTE S.A.S. deberán garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.

La limpieza y aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de un funcionario y/o contratista del Área de Tics. El personal de limpieza debe ilustrarse con las precauciones mínimas a seguir durante el proceso.

Se prohíbe el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
Las actividades de soporte y mantenimiento dentro del centro de datos o central de cableado siempre deben ser supervisadas por un funcionario y/o contratista autorizado por el jefe de TIC's o quien delegue.

Las puertas del centro de datos deben permanecer cerradas.

Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

Los equipos del centro de datos que lo requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center.
- El porte de armas de fuego, cortopunzantes o similares.

- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Todos deben usar los equipos y accesorios asignados y para los fines que se les autorice.

Gestión de Comunicaciones y operaciones.

La oficina TIC's, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura TIC de la Entidad.

Todos los archivos provenientes de equipos externos a la empresa deben ser revisados para detección de virus antes de su utilización dentro de la red de la Entidad.

Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc.), esto compromete la seguridad de los recursos informáticos de la Entidad.

Periódicamente, la oficina TIC's efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de la Entidad.

El jefe del área debe solicitar todos los requerimientos de aplicativos, sistemas, redes, acceso y equipos informáticos mediante soporte de servicios en línea o mesa de ayuda.

Estarán bajo custodia de la oficina de Tics los medios magnéticos/electrónicos (disquetes, CD, discos duros externos, memorias USB u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para

descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

Copias de seguridad

La empresa proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la empresa, los funcionarios no podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información y de acuerdo a los niveles de seguridad establecidos por la Entidad; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

Almacenar la información resultado del ejercicio de las funciones en la carpeta local o servidor de archivos designado por el área de TIC's, de esta forma la entidad generará las copias de respaldo, de lo contrario no queda dentro de la presente política.

El Backup de la información está bajo la responsabilidad de la oficina de TIC's, sin embargo, el usuario debe velar porque éste se realice periódicamente e informar a través de la mesa de ayuda o centro de soporte institucional la incidencia en caso de que no se esté realizando.

La información de la Entidad debe ser respaldada de forma frecuente, almacenada de manera ordenada y debidamente etiquetada en lugares apropiados, en los cuales se pueda garantizar que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

Se debe seleccionar los medios de almacenamiento adecuados de buena calidad para guardar la información de las copias de respaldo, almacenándolas en otra ubicación diferente a las instalaciones donde se encuentra en funcionamiento. El sitio debe ser un sitio externo donde se resguardan dichas copias, cumpliendo con los mismos controles de seguridad adecuados, teniendo en cuenta todas las medidas de protección y seguridad física.

Control de cambios.

Definir los lineamientos para la realización y/o gestión de cambios en los sistemas de información, hardware, redes y aplicativos, estableciendo tanto el método como el procedimiento a seguir para realizar el cambio, las pruebas y las actualizaciones, reduciendo los riesgos de pérdida o daño de información, así como el impacto en la operación de la organización.

Aplica para la realización de pruebas, revisiones, cambios de los aplicativos y softwares desarrollados, se considera el estudio, aprobación, y puesta en marcha de los cambios.

1. Es responsabilidad del coordinador TIC definir los procedimientos a seguir tanto para la solicitud como la realización y aprobación de los cambios, especificando las responsabilidades de cada nivel y área.

2. El equipo de cambios en la organización estará conformado por:

    a. Líder del Área
    b. Coordinador TIC's
    c. Usuarios del aplicativo o software

3. Toda solicitud de cambios debe ser registrada por medio de correo o en la carpeta compartida de ONE DRIVE se debe entregar todos los formatos y estructura de los cambios que requieran.

4. Los cambios tendrán una clasificación de acuerdo con el impacto y prioridad, partiendo de lo más crítico a lo menos crítico, y para lo cual se deberán considerar las variables de riesgo para la operación e impacto. La clasificación utilizará una escala de 1 a 5, en donde 1 es un cambio crítico y urgente para la organización, y 5 es un cambio que puede ser realizado en un período de hasta 3 meses.

5. Todos los cambios clasificados entre 1 y 3 deben ser revisados y autorizados por director de área o líder de área.

6. Se consideran cambios críticos y urgentes, todos aquellos cambios que no siguen el proceso normal de aprobación, dado que no ejecutarlos en el menor tiempo posible, tiene un impacto negativo en la operación normal.

7. Todos los cambios solicitados deben contar con la correspondiente evaluación de riesgos, incluyendo el impacto en la operación, los costos, y el cumplimiento normativo.

8. Los cambios deben ser aprobados formalmente tanto por el director de área o el líder del área a la cual corresponde el cambio, según previa documentación soporte de los cambios y de acuerdo con la aceptación de los resultados del ambiente de pruebas y antes de pasar al ambiente de producción.

Gestión de incidentes de seguridad de la información

El usuario deberá informar a la oficina TIC's a través de herramienta de soporte de servicios en línea o mesa de ayuda, telefónicamente o al correo electrónico soporte@palnortesas.com y al líder inmediato, sobre cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de la Entidad que tenga conocimiento.

Lineamientos para uso de dispositivos móviles

Los dispositivos móviles (teléfonos móviles, computadores portátiles, teléfonos inteligentes (smartphones) tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.

Los usuarios de dispositivos móviles institucionales deben tener instaladas únicamente las aplicaciones distribuidas, autorizadas y configuradas por el administrador de la plataforma.

Los dispositivos móviles asignados por la empresa deben tener la configuración realizada por la oficina TIC's, así mismo solo podrá configurarse únicamente las cuentas de correo electrónico asignadas al usuario por la entidad.

En el caso del nivel directivo se autoriza el uso de WhatsApp únicamente en dispositivos suministrados por la Entidad, no se permite por esta aplicación o cualquiera de envío de

mensajes o correo electrónico, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.

Los dispositivos móviles institucionales deben tener solo la tarjeta SIM asignada por la entidad, igual que la tarjeta SIM solo debe instalarse en los equipos asignados por la entidad.

Los teléfonos móviles y/o teléfonos inteligentes institucionales, debe permanecer encendidos y cargados durante las horas laborales o de acuerdo con la responsabilidad y requerimientos propios del cargo.

El usuario debe usar bien el dispositivo suministrado por la Entidad para realizar actividades propias de su cargo o funciones asignadas en la entidad.

Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.

Los usuarios de dispositivos móviles asignados por la empresa deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).

Los usuarios de dispositivos móviles institucionales deben mantener desactivados las funciones de redes inalámbricas Wifi, puertos infrarrojos, puerto Bluetooth.

Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.

Si se requieren más aplicaciones en el dispositivo móvil institucional, se solicitará al Comité de Gestión y desempeño para su aprobación.

Política de Escritorio limpio

- Todo el personal de la empresa debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.
- Todos los equipos tendrán instalado en su escritorio el fondo de pantalla corporativo autorizado.
- Todo el personal de la empresa debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.
- Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.
- Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. No se deben reutilizar papel con información CONFIDENCIAL.
- En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

Aprobado a los 27 días de junio del 2024

_____

Mauricio Vargas Giraldo
Gerente