POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GREXPHARMA S.A.S

GREXPHARMA S.A.S con **NIT 900618679-9** en el presente documento establece las políticas de seguridad de la información en materia de informática, las cuales se clasifican de la siguiente manera:

ACCESO A LA INFORMACIÓN

Todos los funcionarios y contratistas que laboran para la empresa deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. El representante legal debe autorizar sólo el acceso indispensable al personal de acuerdo con su trabajo.

Todos los accesos y claves de usuarios para el uso de los sistemas de información deberán ser desactivados o cambiados después de que un funcionario, supernumerario o proveedor cese de prestar sus servicios.

ADMINISTRACIÓN DE CAMBIOS

Toda solicitud de mejora de hardware y/o software que afecte los sistemas de información, debe ser requerido por los funcionarios de la empresa que utilizan el sistema.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimientos o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

SEGURIDAD DE LA INFORMACIÓN

Los funcionarios y contratistas de la empresa son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la empresa y por la Ley para protegerla, evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Así mismo no deben suministrar información a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice la infraestructura tecnológica tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está clasificada como confidencial y/o crítica.

SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

El sistema de correo electrónico y servicios web deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades de la empresa.

La propiedad intelectual desarrollada o concebida mientras el funcionario se encuentre en el sitio de trabajo, es propiedad exclusiva de la empresa. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memorandos, planes, estrategias, productos, software, códigos fuentes, documentación y otros materiales.

SEGURIDAD EN RECURSOS INFORMÁTICOS

Los recursos informáticos deben cumplir como mínimo con lo siguiente requisitos:

Administración de usuarios: Establece cómo deben ser utilizadas las claves de ingreso a los recursos informáticos, longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos contables, deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos.

Cada sistema, deberá permitir la asignación a cada usuario de diferentes roles, así como existir un rol para la administración de usuarios.

Registros de auditoría:

El control de acceso a todos los sistemas de computación de la empresa debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las contraseñas o claves de acceso a los recursos informáticos asignados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Toda la información del servidor del software contable que sea sensible, crítica o valiosa debe tener controles de acceso.

SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la empresa, deberán ser considerados y tratados como información confidencial.

Todas las conexiones a redes externas tiempo real que accedan a la red interna, debe pasar a través de un cortafuegos, denominado sistema de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico de información o interacción entre sistemas de información con empresas externas deberá estar autorizado y soportado con un documento de formalización y aprobado por el representante legal.

SOFTWARE UTILIZADO

Todo software que utilice la empresa será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos.

Debe existir una cultura informática al interior de la empresa que garantice el conocimiento por parte de los funcionarios públicos y contratistas de las implicaciones que tiene el instalar software ilegal en los computadores de trabajo que pertenecen a la empresa.

ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la empresa (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación técnica del área de sistemas y aprobación por parte del representante legal.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el área de sistemas.

Los equipos de cómputo (PC, servidores, comunicaciones, etc.) no deben moverse o reubicarse sin la aprobación previa del área de sistemas y el representante legal.

ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad.

El almacenamiento de la información se debe realizar interna y/o externamente, de acuerdo con su importancia

La información de copias de seguridad (BACKUP) en CD-R o DVD-R o DD, debe recaudarla el área de sistemas. Dicho departamento debe darle custodia y consolidación que garantice que la información no sea manipulada por ninguna persona externa o interna durante su transporte.

Las copias de seguridad permitirán hacer seguimiento de control en una auditoría o en caso de requerirse recuperar la información.

CONTINGENCIA

El área de sistemas debe preparar, actualizar y probar anualmente un plan de contingencia que permita a las aplicaciones críticas y otros sistemas de cómputo estar disponibles en un evento de desastre.

Las crisis suelen provocar "reacciones de pánico" que pueden ser contraproducentes y a veces incluso más dañinas que las provocadas por el incidente que las causo.

SEGURIDAD FÍSICA

Las oficinas deben contar con los mecanismos de control de acceso tales como vigilancia privada, identificación de visitantes, sistema de alarmas, etc. En los sitios donde existan sistemas de información, equipos de cómputo y comunicaciones que sean considerados como críticos, deberán contar mínimo con seguridad de acceso con guardia 7x24x365, sistemas de detección y extinción de incendio y circuito cerrado de televisión con cámaras.

Los centros de cómputo o áreas que la empresa considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá estar acompañada permanentemente de un funcionario de la empresa.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

ESCRITORIOS LIMPIOS

Sobre los escritorios u oficinas abiertas y durante la ausencia de los funcionarios no deben permanecer a la vista documentos en papel, dispositivos de almacenamiento como CDs, memorias USB y/o discos duros, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

ADMINISTRACIÓN DE LA SEGURIDAD

Cualquier brecha en la seguridad o sospecha en la mala utilización en el Internet, la red Intranet, o los recursos informáticos, debe ser comunicada por el funcionario que la detecta en forma inmediata y confidencial al área de sistemas y representante legal.

Los funcionarios y contratistas que realicen las labores de administración del recurso informático son responsables por la implementación y permanencia de los controles sobre los recursos tecnológicos.

PRÁCTICAS DE USO DE INTERNET

Los virus informáticos son los principales riesgos de seguridad para los sistemas de información, por

tal razón se deben tomar las siguientes precauciones de seguridad sobre la utilización de Internet:

1. No utilizar canales de chat o grupos sociales como Facebook, Messenger, etc, en horario laboral con fines personales.
2. No descargar de Internet, ni alojar en los discos duros de los equipos de trabajo, música, videos, ni cualquier tipo de software sin licenciamiento.
3. No abrir ningún mensaje, sitio web, ni archivo de fuente desconocida. En caso de personas conocidas, se deben tomar precauciones, asegurándose de que esa persona es la responsable del envío y ante cualquier duda, borrar el mensaje, para evitar la contaminación de un virus.
4. Todos los funcionarios tienen la obligación a dar cumplimiento a la Ley 679 de 2001, acatando las prohibiciones que le han sido impuestas. Por consiguiente, se obligan a no utilizar los servicios, redes y sistemas que impliquen directa o indirectamente, bajar o consultar información de actividades sexuales y/o material pornográfico.
5. El spam o correo basura son los mensajes no deseados que hacen referencia a publicidad pudiendo además contener virus; estos mensajes deben eliminarse sin ser leídos para evitar el aumento de la cantidad del correo basura en el buzón, así como la posibilidad de intrusión de virus en el sistema.
6. Usar regularmente un programa antivirus y verificar periódicamente su actualización. El área de sistemas deberá prestar el soporte que se requiera para tal fin.
7. No bajar nada de sitios web de los que no se tenga referencias de seriedad, o que no sean medianamente conocidos. Si se bajan archivos, copiarlos a una carpeta y revisarlos con un antivirus actualizado antes de abrirlos.
8. Se debe suministrar el correo electrónico asignado por la empresa con moderación, ya que podrían enviar publicidad no deseada.

9. No utilizar la cuenta de correo electrónico suministrada por la empresa, para asuntos personales.

10. Activar las actualizaciones automáticas de software.