NORMAS Y POLÍTICAS

POLÍTICA DE CONTROL DE ACCESOS

Aprobado por:	*Nombre: Pedro Ospino* *Cargo: Gerente de TI* *Fecha: 21/01/2019*

REGISTRO DE CAMBIOS

Revisión	Fecha	Responsable	Descripción del Cambio

LISTA DE DISTRIBUCION

DOCUMENTO CONTROLADO. NO COPIAR **SOLO PARA USO INTERNO**

1. PROPÓSITO

PRIXMASOL es una empresa comprometida en proteger la seguridad y la privacidad de información, así como de garantizar la continuidad de los procesos clave del negocio a través del uso de las mejores prácticas de Seguridad de Información y en cumplimiento con las leyes, regulaciones aplicables y requerimientos de la industria.

A través de su Política de seguridad de TI, PRIXMASOL busca proteger el acceso no autorizado a sus activos críticos de cualquier amenaza interna, externa, accidental o deliberada que pongan en riesgo la confidencialidad, disponibilidad e integridad de su información.

2. ALCANCE

Aplica para todo el personal y proveedores que utilicen recursos del Área de TI o información que pertenece a PRIXMASOL.

Aplica para cualquier tipo de activo y sistema de información propiedad de PRIXMASOL.

Aplica sobre toda información (oral, impresa, electrónica y visual) propiedad de PRIXMASOL y sus empresas filiales o cedidas a ellas, generada y/o manejada por trabajadores permanentes o temporales, contratistas, personal bajo convenio de asistencia tecnológica, tesistas, aprendices y pasantes.

3. ÁREAS INVOLUCRADAS

Participación activa de la Gerencia de Seguridad de Información y Riesgos TI, Gerencia de Infraestructura, Tecnología de Información, e involucra a toda la Organización.

4. NORMAS Y POLÍTICAS

4.1. Control de Acceso

- El acceso a los sistemas críticos de información de PRIXMASOL se otorga los privilegios mínimos y necesarios para la óptima ejecución de sus funciones en el negocio.

- La asignación de accesos y permisos a los activos críticos de información de PRIXMASOL se ejecuta a través de un proceso formal de autorización por parte del dueño y custodio de los sistemas y aplicaciones.
- Cada empleado de PRIXMASOL debe contar con un usuario y contraseña únicos para su acceso a los activos críticos de información. Queda prohibido el compartir o intercambiar contraseñas con otros empleados, contratistas, proveedores y/o clientes.
- Cada cuenta de usuario, permiso o acceso a sistemas de información (aplicaciones, red, correo, etc.) se debe relacionar con un responsable único.
- Deberá seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- Reportar inmediatamente a su jefe inmediato o a la Gerencia Seguridad de Información y Riesgo de TI cualquier evento que pueda comprometer el usuario ó Password, el acceso no autorizado a un activo de información.
- Cualquier cambio de estatus laboral de los empleados de PRIXMASOL (terminación voluntaria, transferencia, promoción o despido) será registrado y comunicado por Recursos Humanos a la Gerencia de Seguridad y Riesgo TI, con la finalidad de revisar y actualizar de manera periódica el control de acceso a los sistemas críticos e instalaciones de PRIXMASOL.
- Todos los empleados, contratistas y proveedores que tienen acceso a los sistemas de información son sujetos al cumplimiento de los requerimientos de seguridad definidos en la *"Política de Control de Accesos".*
- La Gerencia de Seguridad de Información y Riesgo de TI es la responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas. La Gerencia de Seguridad de Información y Riesgo de TI también es responsable de informar al Vicepresidente de Tecnología de Información y Tecnología sobre toda actividad sospechosa.
- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

4.2. Creación de Accesos

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- La solicitud de una nueva cuenta o el cambio de privilegios debe seguir los procedimientos de creación, eliminación y movimiento de usuarios que se establezcan.
- No debe concederse una cuenta a personas que no sean empleados de PRIXMASOL a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al terminar sus labores dentro de la Organización.
- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento, ni permitir su acceso remoto a menos que el Gerente de Seguridad de Información y Riesgo de TI determinen que sea necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo. Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, o certificados digitales.
- Se prohíbe el uso de cuentas anónimas o de invitado (Guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas deben emplear su propio ID y luego obtener el acceso como Administrador. En cualquier caso debe registrarse en la bitácora todos los cambios de ID.
- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
- Cuando un empleado es despedido o renuncia a PRIXMASOL, debe desactivarse su cuenta antes de que deje el cargo.

4.3. Contraseñas y el control de acceso

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, debe obligarse a que el usuario deba escoger otra contraseña.
- Deben implementarse los mecanismos necesarios para obligar al cambio de contraseña en los sistemas en un tiempo recomendado de 30 días.
- Las contraseñas predefinidas que traen los equipos nuevos, deben cambiarse inmediatamente al ponerse en servicio el equipo.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto, la sesión debe ser inmediatamente desconectada.
- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 10 minutos. El reestablecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo).
- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de PRIXMASOL, pudiendo ser causal de despido.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
- Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón, deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.
- A fin de proteger las contraseñas con altos privilegios o con condiciones especiales se deben implementar mecanismos de protección para las mismas, como encriptación, certificados ó métodos biométricos que complementen las mismas.
- Los servidores de red y los equipos de comunicación deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

4.4. Monitoreo de Acceso y Uso de Sistemas de Información

- PRIXMASOL se reserva el derecho de monitorear y auditar la infraestructura de telecomunicaciones, telefonía, correo electrónico y equipos de cómputo propiedad de PRIXMASOL con la finalidad de detectar cualquier actividad sospechosa y/o uso indebido de sus activos de información.
- Únicamente personal autorizado y designado por el CSI (Comité de Seguridad de la Información) podrá llevar a cabo funciones de monitoreo las cuales podrán ser auditadas y monitoreadas respectivamente.
- Los resultados del monitoreo de actividad sospechosa o de uso inadecuado de los sistemas, deberá ser notificado a personas autorizadas de PRIXMASOL para la aplicación de sanciones o la medidas disciplinarias correspondientes.

- El staff autorizado por el CSI de PRIXMASOL podrá revisar la actividad y cuentas de usuario incluyendo archivos, sesiones, contenido de las comunicaciones y de acceso a Internet sin notificación previa al empleado o contratista bajo los siguientes criterios:
  - Exista una cuenta que restringa el acceso a los equipos de cómputo y recursos de la red a otros usuarios de la red.
  - Patrones generales del uso de una cuenta indican que existen actividades no aceptables o no autorizadas.
  - Existe evidencia razonable para creer que el usuario ha violado o está violando la política de seguridad o de la ley.
  - Se requiere para cuestiones de proteger la responsabilidad laboral y jurídica de la compañía
  - Se requiere por cuestiones de cumplimiento de la ley y regulaciones aplicables.
- Cuando se descubra evidencia de actividad criminal o sospechosa, tales como material en formato impreso o electrónico de archivos, correos y/o bitácoras se turnarán al personal autorizado y apropiado de PRIXMASOL para el manejo responsable de esta información y aplicación de las medidas disciplinarias correspondientes.

4.5. Sanciones

La inobservancia de esta política es considerada como una falta grave y dependiendo de la magnitud del incumplimiento, se hará entrega de notificación de falta.

4.6. Excepciones

Cualquier aspecto relacionado con la Clasificación de la Información, que no esté contemplado en la presente política, será evaluado en forma particular por el Comité de Seguridad de la Información y debidamente documentado y autorizado.

4.7. Actualizaciones

- Esta política deberá ser revisada anualmente por los responsables de su cumplimiento para actualizarla y cumplir con los requerimientos nuevos en materia de Seguridad y Riesgos de TI.
- Se realizarán revisiones y actualizaciones cuando se solicite por parte del comité o sea meritoria.

5. RESPONSABLES

Los responsables que deberán hacer cumplir esta política son:

- Gerencia de Seguridad y Riesgos TI
- Gerentes y Directores de PRIXMASOL

5.1. Es responsabilidad de Seguridad de TI:

- Supervisar el desarrollo y el cumplimiento de políticas y procedimientos de Control de Accesos de PRIXMASOL, así como asegurar su mantenimiento, actualización y revisión de las mismas a través del CSI (Comité de Seguridad de la Información).
- Identificar los lineamientos, procedimientos y políticas aplicables de PRIXMASOL para el control y acceso de su información.
- Administrar el recurso asignado por el CSI (Comité de Seguridad de la Información) para la implementación de los controles y prácticas de seguridad necesarias para mitigar los riesgos identificados en el acceso a la información ó recursos tecnológicos.
- Vigilar y trabajar cercanamente con los dueños y custodios de la información para coordinar los esfuerzos de seguridad a lo largo de la compañía, incluyendo Tecnología de información, Recursos Humanos, Legal, y otros grupos que apoyen en la implementación de estándares e iniciativas de seguridad.
- Administrar la capacitación y concientización continua que permita que cualquier persona independiente de su estatus (empleado, contratista, personal externo, practicante, proveedor, representante, etc.) conozca las políticas, prácticas y procedimientos vigentes para el correcto manejo de la seguridad de información y accesos en PRIXMASOL.
- Coordinar y supervisar los recursos asignados para la implementación, monitoreo, documentación y comunicación de los requerimientos de Seguridad de la Información para PRIXMASOL.
- Monitorear y reportar periódicamente el cumplimiento de los controles y políticas de seguridad de TI definidos por PRIXMASOL y asegurar la identificación e implementación de las acciones correctivas.

5.2. Es responsabilidad del Dueño de la Información:

- Identificar los requerimientos legales y regulatorios que el manejo de su información debe cumplir.

- Determinar la clasificación y el control de acceso a la información.
- Aprobar o rechazar las solicitudes de "acceso" a la información.
- Determinar los roles de acceso para soportar el "Principio de Mínimo Privilegio" y de "Segregación de funciones".
- Seleccionar controles de seguridad de información con el responsable de Seguridad de TI.
- Seleccionar la opción de tratamiento de riesgos (Aceptar / Evitar / Transferir / Mitigar).

5.3. Es responsabilidad del Custodio de la información:

- Asegurar el cumplimiento de todas las políticas y requerimientos de seguridad y Control de Accesos de PRIXMASOL.
- Soportar el control de acceso a la información, actuando como un punto de control único para todas las peticiones de acceso autorizadas por el dueño de la información.
- Soportar los procedimientos de control y revisiones regulares que aseguren que todos los usuarios y accesos privilegiados son los autorizados y se encuentran vigentes.
- Asegurar que el acceso autorizado a los usuarios está basado en el "Principio de menor privilegio" y "Principio de segregación de funciones."
- Administrar el cumplimiento y la efectividad de los controles de seguridad definidos por el dueño de información.

5.4. Es responsabilidad de los Gerentes de todas las áreas de PRIXMASOL:

- Promover y supervisar el cumplimiento efectivo de las políticas y procedimientos de seguridad aplicables a su staff y personal que labora bajo su responsabilidad, así como de reportar inmediatamente al responsable de Seguridad de TI cualquier actividad o situación que por incumplimiento ponga en riesgo la operación del negocio.
- Asegurar que el personal a su cargo participe en las campañas de concientización entrenamiento de seguridad e información.
- Para el caso de los gerentes de TI, deberán participar en el proceso de de administración de riesgo y seguimiento a los controles identificados para la reducción de brechas de seguridad.

5.5. Es responsabilidad del Usuario de la información:

- El personal con acceso a la información de PRIXMASOL deberá de actuar con discreción, sentido común y con juicio razonable durante la creación, almacenamiento, procesamiento, transmisión o desecho de la Información utilizada durante la ejecución de sus actividades, independientemente del medio en el cual se encuentre contenida dicha información.
- Cualquier persona independiente de su relación laboral con PRIXMASOL (contratista, personal externo, practicante, proveedor, representante, etc.) deberá cumplir con los lineamientos establecidos en la presente Política de Control de Acceso para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información de PRIXMASOL.
- Apoyar en el cumplimiento de las leyes y regulaciones aplicables.
- Cumplir con todas las políticas, procedimientos y lineamientos de seguridad aplicables.
- Proteger y nunca compartir las cuentas de acceso y contraseñas con terceros.
- Mantener la confidencialidad de información crítica a la cual tiene acceso.
- Aceptar la responsabilidad de todas las actividades asociadas con el uso de sus cuentas de usuario y privilegios de acceso relacionados.
- Reportar toda la actividad sospechosa y/o violaciones a la Política de Seguridad de TI a las autoridades correspondientes (gerentes, supervisores, administradores de sistemas o al responsable de Seguridad de TI).

5.6. Es responsabilidad del personal externo:

- Tendrá las mismas responsabilidades que los empleados de PRIXMASOL, además de tener un documento firmado de confidencialidad de información administrado por el Departamento de Legal de PRIXMASOL.

6. REGISTROS Y/O FORMULARIOS

- N/A

7. PROCEDIMIENTO Y FLUJOGRAMAS

- N/A

8. DOCUMENTOS Y LINKS DE REFERENCIA

- Política de Clasificación de información
- Política de Control de Acceso

9. GLOSARIO

- CSI: (Comité de Seguridad de la Información).
- Usuarios: son las personas que requieren de la "autorización" del dueño de la información para poder accederla y poder realizar sus funciones a través de los recursos que le fueron asignados.