POLÍTICA DE CONTROL DE ACCESO DE DATOS	PRO-08
	Revisión 00

REV.	FECHA	DESCRIPCIÓN

ELABORADO POR: Carlos J. Pérez Aguilera	REVISADO Y APROBADO POR: DIRECCIÓN
FECHA:	

POLÍTICA DE CONTROL DE ACCESO DE DATOS	PRO-08
	Revisión 00

ÍNDICE

1.-OBJETO

POLÍTICA DE CONTROL DE ACCESO DE DATOS	PRO-08
	Revisión 00

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

Los usuarios de este documento son todos los empleados de la empresa

2.-ALCANCE

Este procedimiento es aplicable a todo el personal de la empresa.

3.-DEFINICIONES

No aplica

4.-DEFINICIONES

Control de acceso

4.1. Introducción

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Está permitido el acceso a todos los sectores físicos de la organización, excepto a aquellos para las cuales el privilegio debe ser concedido por una persona autorizada (punto "Gestión de privilegios").

Esta Política determina reglas de acceso a sistemas, servicios e instalaciones, mientras que la Política de clasificación de información define reglas de acceso para documentos y registros individuales.

4.2. Perfil de usuario A

El perfil de usuario A tiene los siguientes derechos de acceso:

Nombre del sistema / red / servicio	*Derechos de usuario*
Archivo físico en papel e informatizado de clientes y proveedores (Software de gestión comercial)	Lectura / Escritura
Archivo físico en papel e informatizado de trabajadores	Lectura / Escritura

Los siguientes cargos tienen derechos de acceso de acuerdo al Perfil de usuario A:

Dirección
Administración

4.3. Perfil de usuario B

El perfil de usuario B tiene los siguientes derechos de acceso:

Nombre del sistema / red / servicio	*Derechos de usuario*
Archivo físico en papel e informatizado de clientes y proveedores (Software de gestión comercial)	Consulta
Archivo físico en papel e informatizado de trabajadores	Consulta

Este perfil de usuario se concede a todos los empleados al momento de ser contratados.

Los siguientes cargos tienen derechos de acceso de acuerdo al Perfil de usuario B:

Empleados en general

4.4. Gestión de privilegios

POLÍTICA DE CONTROL DE ACCESO DE DATOS	PRO-08
	Revisión 00

Los privilegios respecto de los perfiles de usuario mencionados anteriormente (concesión o eliminación de derechos de acceso) son asignados de la siguiente forma:

Nombre del sistema / red / servicio / sector físico	***Quién está autorizado a conceder o eliminar derechos de acceso***	***Forma del proceso de autorización***
Archivo físico en papel e informatizado de clientes y proveedores (Software de gestión comercial)	Responsable de Seguridad	Por escrito
Archivo físico en papel e informatizado de trabajadores	Responsable de Seguridad	Por escrito

4.5. Revisiones periódicas de los derechos de acceso

Los propietarios de cada sistema y de las instalaciones para los cuales se requieren derechos de acceso especiales deben, según los siguientes intervalos, revisar si los derechos de acceso concedidos se mantienen de acuerdo a los requerimientos de negocios y de seguridad:

Nombre del sistema / red / servicio / sector físico	***Intervalos para revisiones periódicas***
Archivo físico en papel e informatizado de clientes y proveedores (Software de gestión comercial)	Una vez al año
Archivo físico en papel e informatizado de trabajadores	Una vez al año

Cada revisión debe ser registrada en un acta o informe que se debe reportar al Responsable de Fichero.

4.6. Cambio de estado o finalización de un contrato

Cuando se produce un cambio o finalización de empleo, el Responsable de Seguridad debe informar inmediatamente a la persona que autorizó los privilegios del empleado en cuestión.

Cuando se modifican las relaciones contractuales con entidades externas que tienen acceso a sistemas, servicios e instalaciones, o cuando finaliza el contrato, el propietario del contrato debe informar inmediatamente a las personas que autorizaron los privilegios de las entidades externas en cuestión.

Los derechos de acceso para todas las personas que han modificado su condición de empleo o relación contractual deben ser eliminados o modificada inmediatamente por las personas responsables de acuerdo a lo que se define en la siguiente sección.

4.7. Implementación técnica

La implementación técnica de la asignación o eliminación de derechos de acceso la realizan las siguientes personas:

Nombre del sistema / red / servicio / sector físico	***Persona responsable de la implementación***
Archivo físico en papel e informatizado de clientes y proveedores (Software de gestión comercial)	Responsable de Seguridad
Archivo físico en papel e informatizado de trabajadores	Responsable de Seguridad

Las personas detalladas en este cuadro no pueden asignar ni eliminar libremente los derechos de acceso, sino solamente en base a los perfiles de usuario definidos en la presente Política y a solicitudes de personas autorizadas para asignar privilegios.

4.8. Gestión de la clave del usuario

POLÍTICA DE CONTROL DE ACCESO DE DATOS	PRO-08
	Revisión 00

Cuando se asignan y utilizan claves de usuarios, se deben cumplir las siguientes reglas:

Al firmar la Declaración de aceptación de los documentos del SGSI, los usuarios también aceptan la obligación de mantener sus claves en forma confidencial, como se establece en este documento.
Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos corresponda.
Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo informado anteriormente.

Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario

El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez.

El sistema de gestión de claves debe requerir que el usuario escoja contraseñas seguras.
El sistema de gestión de claves debe requerir que los usuarios cambien sus claves cada tres meses.
Si el usuario solicita una nueva clave, el sistema de gestión de claves debe determinar la identidad del usuario mediante su nombre de usuario. (pueden realizarse acciones como, por ejemplo, enviando un correo electrónico instruyendo al usuario para que realice una acción, etc.
El usuario debe confirmar la recepción de la clave, ingresando al sistema dentro de un intervalo de tiempo determinado, etc.
La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
Si un usuario ingresa una clave incorrecta tres veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión.
Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.
Los archivos que contienen claves deben ser guardados en forma separada de los datos de sistema de la aplicación.

5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS

POLÍTICA DE CONTROL DE ACCESO DE DATOS	PRO-08
	Revisión 00

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Registro de asignación de privilegios	Carpeta RGPD	Responsable de Seguridad	Los registros no pueden ser editados, sólo el Responsable de Seguridad puede guardar estos registros	Los registros son almacenados por el plazo de 3 años.
Registros de la revisión habitual de los derechos de acceso	Carpeta RGPD	Responsable de Seguridad	Solamente el Responsable de Seguridad tiene derecho de acceso a estos registros.	Los registros son almacenados por el plazo de 3 años.