Titulo:

Seguridad del Sistema

	PUESTO	NOMBRE	FECHA
ELABORADO POR:	Jefe de Sistemas	Erwin Velasquez	31/08/2023
REVISADO POR:	Jefe de Seguridad y Calidad	Ricardo Alarcón	31/08/2023
APROBADO POR:	Gerente General	Giovanni Klein	31/08/2023

1. OBJETIVO

Describir las actividades a realizar para la creación de usuarios, mantenimiento y control de claves para accesos a la red y sistemas, además del mantenimiento de los servidores y dispositivos de la red de la Empresa; siguiendo una política de seguridad informática que minimice los riesgos de pérdida o robo de información.

2. ALCANCE

Incluye a los diferentes sistemas utilizados y la asignación de usuarios.

3. RESPONSABILIDAD

El ***Jefe*** de Sistemas es el responsable de la correcta aplicación del presente procedimiento.

4. ABREVIATURAS

No Aplica

5. REFERENCIAS

5.1. Norma Internacional ISO 9001
5.2. Norma y Estándar Internacional BASC
5.3. Norma Técnica Peruana NTP ISO 37001

6. DEFINICIONES

No Aplica

7. CONDICIONES GENERALES

No Aplica

8. DESCRIPCION DEL PROCEDIMIENTO

8.1. Claves:

a. El Asistente de ***Soporte*** es el responsable de proporcionar la clave de acceso a los distintos recursos informáticos disponibles, para establecer una alta seguridad informática del Sistema.
b. Cada usuario debe contar con un “username” y una clave para poder acceder a la red y a los sistemas de la Empresa.
c. Cada usuario puede ingresar al servidor principal y utilizar los sistemas dependiendo del nivel de acceso de su “username” y de las funciones del mismo.
d. La clave de acceso debe tener ***como mínima 08*** caracteres.
e. La clave de acceso al usuario de PC asignada deberá ser modificada mínimo 02 veces al año.
f. Al finalizar el vínculo laboral del trabajador, se invalida el username del usuario y todos sus accesos a los sistemas.

8.2. Hardware:

a. Para la protección de equipos de alto riesgo, contamos con un UPS en el Departamento de Sistemas que protege a los servidores y dispositivos de red y comunicación ante eventuales cortes de energía eléctrica.
b. El edificio cuenta con un grupo electrógeno para hacer funcionar las PC ’s de la red y de esta forma la operatividad no se detenga.
c. El servidor principal de la Empresa cuenta con una fuente de poder redundante y también posee un arreglo de discos (RAID 5) para mayor protección de la información.

8.3. Seguridad de la información:

a. En la mayoría de los casos, los discos lógicos (drives), mayores a E, están ubicados en alguno de los servidores de la Empresa, los demás (A, B, C, D y E) corresponden a discos locales. Se encuentran deshabilitados los puertos para la utilización de dispositivos USB, encargándose el área de Sistemas de habilitarlos únicamente en los casos que la Gerencia General lo estime

conveniente.

b. Sólo se realizará la copia de respaldo (Backup) de la información almacenada en los discos ubicados en los servidores y en la carpeta BKP_SISTEMAS instalada para cada usuario. El área de Sistemas no se responsabiliza por ningún archivo que se encuentre en discos locales, cuya copia de respaldo será de exclusiva responsabilidad del usuario de la PC.
c. Cualquier acción que realice un trabajador de la organización, en perjuicio de la seguridad del sistema, la información o los equipos, será considerado como una falta grave y le corresponderá las sanciones estipuladas en el Reglamento Interno de la empresa.

8.4. Contingencias Informáticas:

a. El tratamiento y las acciones a tomar para los casos de contingencias que podrían presentarse, tales como la falta de fluido eléctrico, interrupción del servicio de correos electrónicos e internet, fallas en los programas o aplicaciones o pérdida de la información se indican en el PRO-TI-007 Procedimiento de Contingencias Informáticas.

8.5. Control del acceso a la información:

a. Se debe tener un buen control del acceso a los equipos y de la información del sistema, incluso los días que no labora el total de trabajadores.
b. Revisar periódicamente los accesos asignados a los usuarios.
c. Se programa el bloqueo de la sesión de equipos desatendidos pasado los 10 minutos.
d. Las Jefaturas indicarán mediante un correo, la relación de personas que han sido designadas para laborar el sábado.
e. El personal que tiene un turno de trabajo el día sábado o que por alguna razón ha necesitado trabajar ese día, debe marcar su ingreso y salida de la oficina en el reloj biométrico que registra el ingreso y salida del personal.
f. Si se detecta que ha ingresado un trabajador no declarado, se informará a RRHH para que tome las medidas que corresponda.

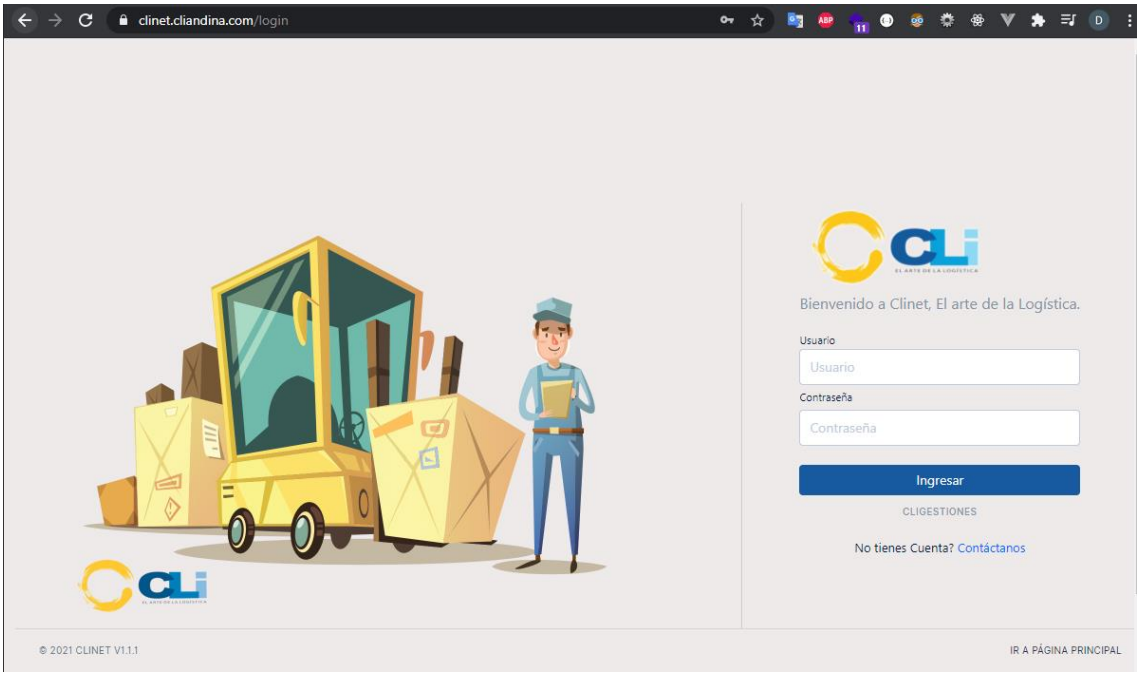
8.6. Cambio de clave CLINET:

En CLINET, se ha implementado la funcionalidad de cambiar la clave cada 90 días. A continuación, se detallan los puntos del proceso.

a. Para comenzar con todo el proceso, primero se debe de cambiar la contraseña obligatoriamente por primera vez. Al momento de ingresar a CLINET con el usuario y clave, se mostrará la siguiente pantalla para ingresar su nueva clave.

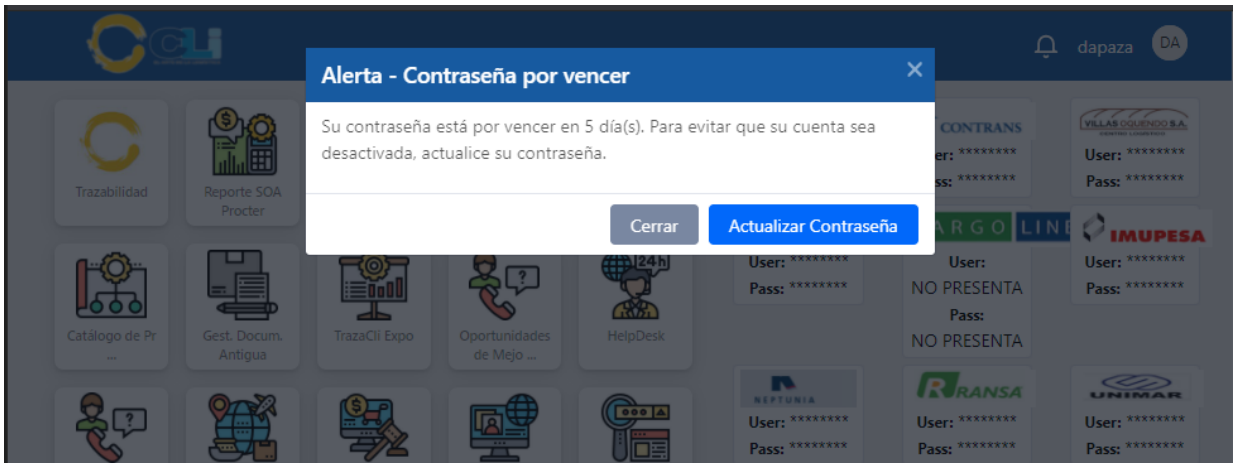
- Contraseña Actual: Se debe ingresar la calve actual del usuario CLINET que será reemplazado.
- Nueva Contraseña: Se debe ingresar la nueva clave. Esta debe de tener por lo menos 6 caracteres y debe de contener por lo menos una letra y un número.
- Confirmar Nueva Contraseña: Se debe ingresar la misma nueva clave.

b. Una vez ingresado los datos solicitados, al presionar “Cambiar Contraseña” se redireccionará nuevamente a la pantalla de LOGIN para ingresar con su nueva clave.



c. Así también, se enviará un correo al usuario por el cambio de clave.

d. Desde ese momento, se considerarán 90 días para el próximo cambio de clave, para lo cual, faltando 5 días para el vencimiento, se notificará al ingresar a CLINET, que se debe de realizar el cambio de clave.



Esta alerta en CLINET, se mostrarán los últimos 5 días hasta el vencimiento de la clave. Se debe de presionar el botón “Actualizar Contraseña” para repetir todo el proceso anteriormente mencionado.

De hacer caso omiso a esta alerta, y no actualizar la clave, la cuenta será bloqueada y se le notificará del bloqueo por correo a la jefa del área correspondiente.

9. CONTROL DE CAMBIOS

9.1. Se ha modificado el ítem **3. RESPONSABILIDAD:** El ***Jefe*** de Sistemas es el responsable de la correcta aplicación del presente procedimiento.

9.2. Se han modificado los siguientes ítems:

- 8.1.a. El Asistente de ***Soporte*** es el responsable de proporcionar la clave de acceso a los distintos
- 8.1.d. La clave de acceso debe tener ***como mínima 08*** caracteres.

9.3. Se han incluido en el ítem **10. ANEXOS**:

- ***FOR-SIG-073 Registro de Capacitación***
- ***FOR-TI-006 Formato de Conformidad_CLI GEST***
- ***FOR-TI-007 Formato de Conformidad_CLI PROY***

10. ANEXOS

10.1.FOR-SIG-073 Registro de Capacitación

10.2.FOR-TI-041 Mantenimiento de Equipos de Cómputo.

10.3.FOR-TI-006 Formato de Conformidad_CLI GEST

10.4.FOR-TI-007 Formato de Conformidad_CLI PROY