

APP Compliance

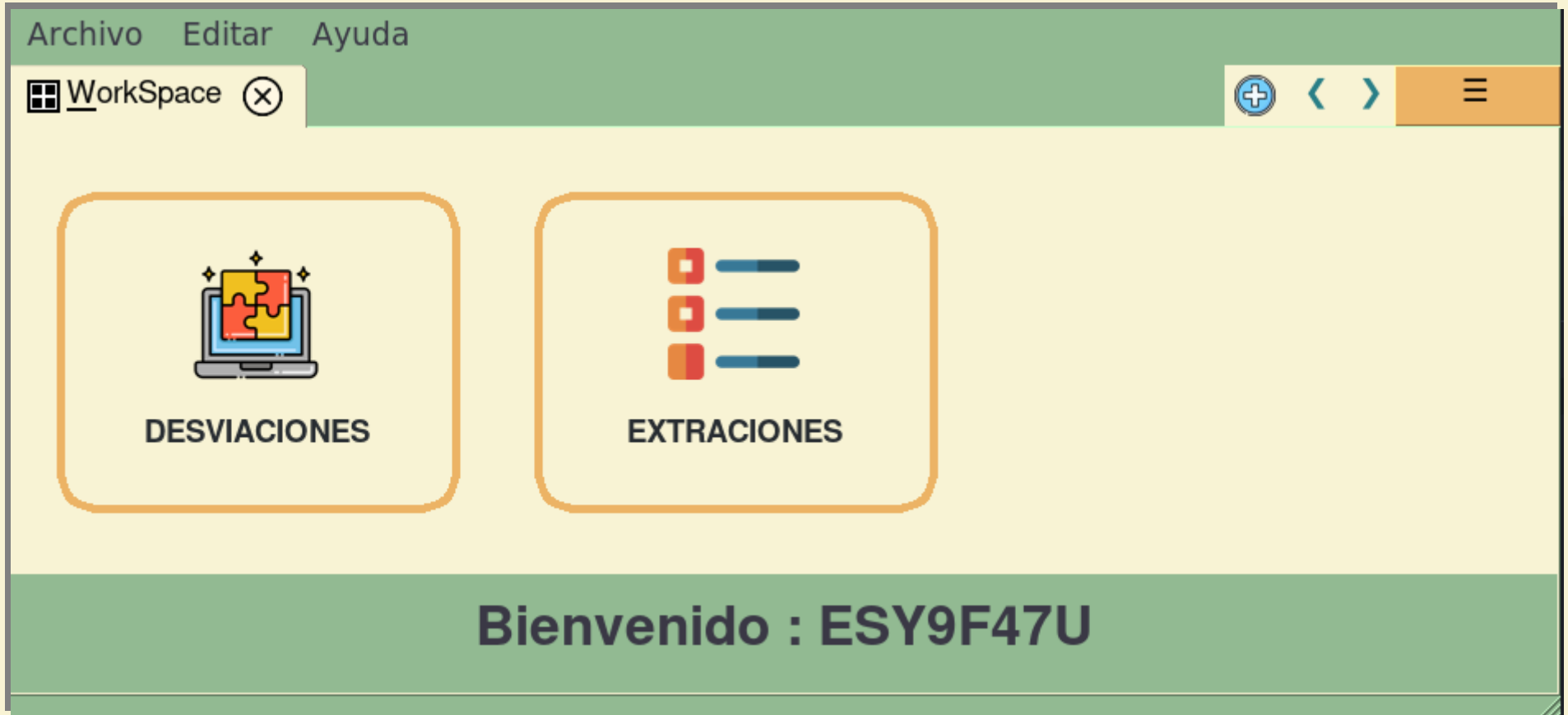
Version 2.5

Aplicación para Análisis y Soluciones de issues health checking para clientes.

- Extracciones
- Desviaciones

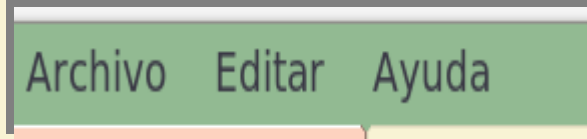
La APP Compliance trata de simplificar errores de extracción, aumentar la respuesta de trabajo y el flujo de trabajo, el poner tener una sola información para todos los clientes, esta diseñada para que sea ágil y rápida y tener las instrucciones a la hora de implementar una configuración en los servidores, mantener datos que sean claros y precisos, para evitar vulnerabilidades en los servidores por un mala configuración.

Workspace



Workspace

- Barra de Menú

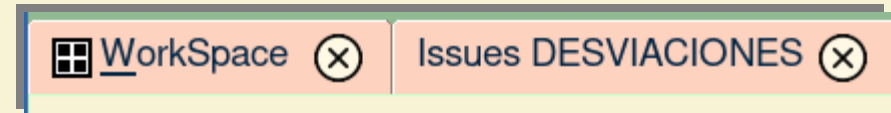


- Área de Botones

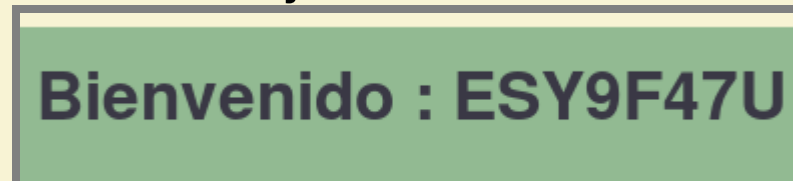


Se compone de...

- Barra de Pestañas



- Mensaje de Bienvenida



Workspace

Barra de Menú

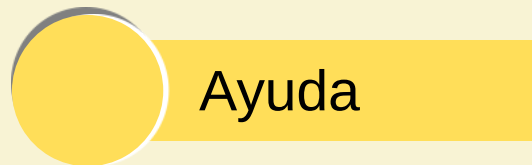
Archivo Editar Ayuda



Esta compuesto con un submenú, para abrir el tipo de issues, ya sea extracción o desviación, ademas de seleccionar el cliente que deseamos revisar y un botón de salir.



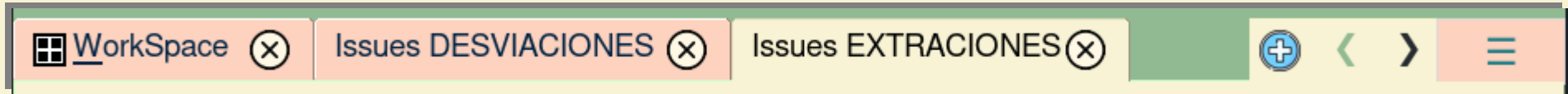
Esta compuesto con un submenú, para poder buscar el modulo a revisar.




Esta compuesto con un submenú, acerca de para poder saber la versión de la APP y ademas un pequeño diccionario de ayuda con palabras claves y módulos relacionados y facilitar la búsqueda de módulos


Workspace


Barra de Pestañas



En la barra de pestañas, podremos tener tantas pestañas abiertas como clientes o tipo de issues que queramos revisar.

- Además tenemos un botón de añadir nueva pestaña. 

- Podremos avanzar en el panel de pestañas, cuando el panel contenga muchas pestañas. 

- Contenedor de pestañas, que estarán todas las pestañas abiertas, donde se podrá elegir la pestaña y movernos a su posición. 

Workspace



Area de Botones

En esta área de botones, actualmente consta de 2 botones, para abrir el espacio de trabajo para issues de extracciones y desviaciones, se puede añadir mas botones dependiendo las necesidades.

Workspace

Mensaje de Bienvenida

Bienvenido : ESY9F47U

En esta parte nos muestra un saludo de bienvenida al usuario que ha iniciado la aplicación

ÁREA DE EXTRACCIONES

The screenshot displays a software interface with two main panels. The left panel, titled 'FICHEROS de EXTRACCIONES', shows a hierarchical file structure. The right panel is a text editor showing the content of a file named 'SSH_Linux_INFRA_Base_P...'. The text in the editor includes a search command, a 'CONTESTAR YES' section, and 'AV.1.1.5 Password Requirements'.

FICHEROS de EXTRACCIONES

- ▷ IDISO
- ▷ LBK
- ▷ FT
- ▷ PLANETA
- ▼ INFRA
 - ▷ Aix
 - ▷ Samba
 - ▷ Hmc
 - ▷ Vios
- ▼ Linux
 - OS_Linux_INFRA_7&8(noIF)
 - OS_Linux_INFRA_Base_PRI
 - OS_Linux_INFRA_Base_PRI
 - OS_Linux_INFRA_ITss_REH
 - SSH_Linux_INFRA_Base_P
 - SSH_Linux_INFRA_Base_P

~ 3 de 9 ~

AV.1.1.

find /home/*/.ssh -name id_rsa|while read fil; do echo \$fil; head \$fil|grep -v ENCRYPTED; done

/* **CONTESTAR YES** */ : " Si las claves privadas pertenecen al owner y tienen una frase de paso.

/* **CONTESTAR NO** */ : " SSH Private Key: \$file_idrsa not passphrase protected

---**AV.1.1.5 Password Requirements**

"Private Key Passphrases

// Nos habla de la características de la Passphrases

// Las frases de contraseña deben tener un número mínimo de 15 caracteres. Todas las demás reglas de contraseña son aplicables.

---**AV.1.1.6 Password Requirements**

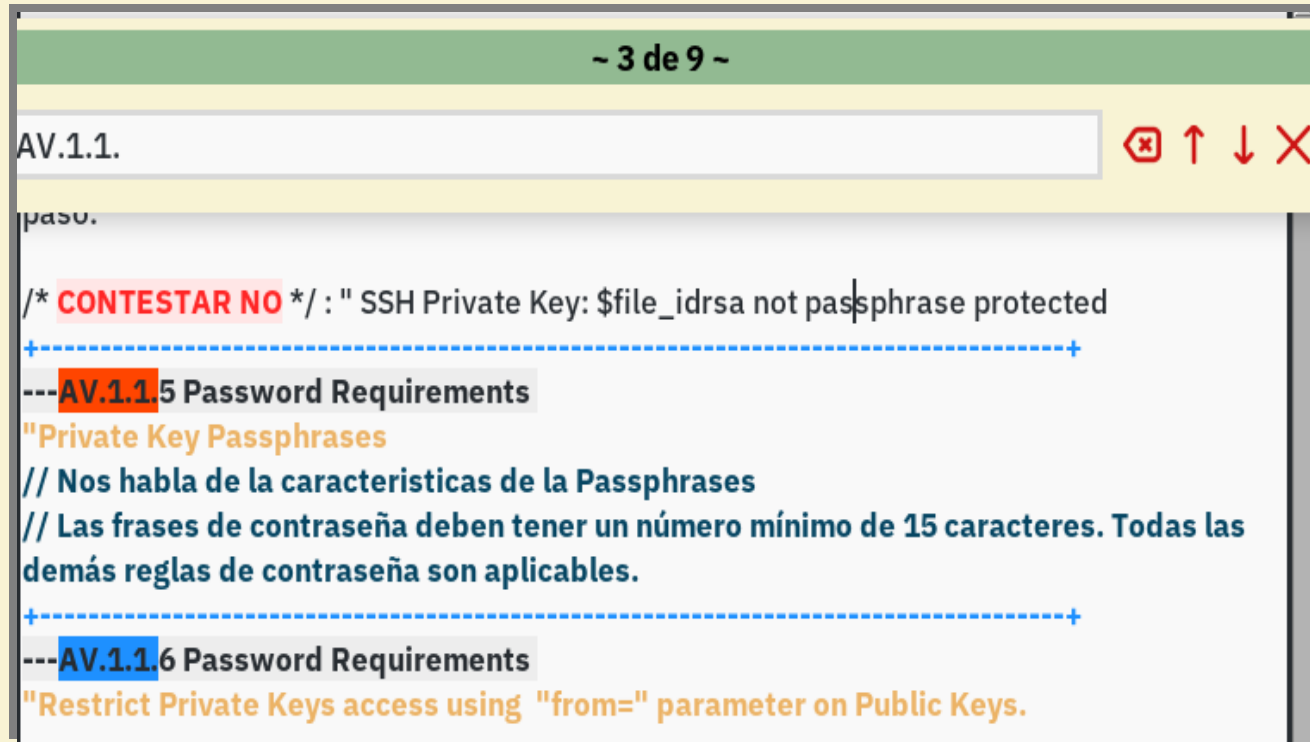
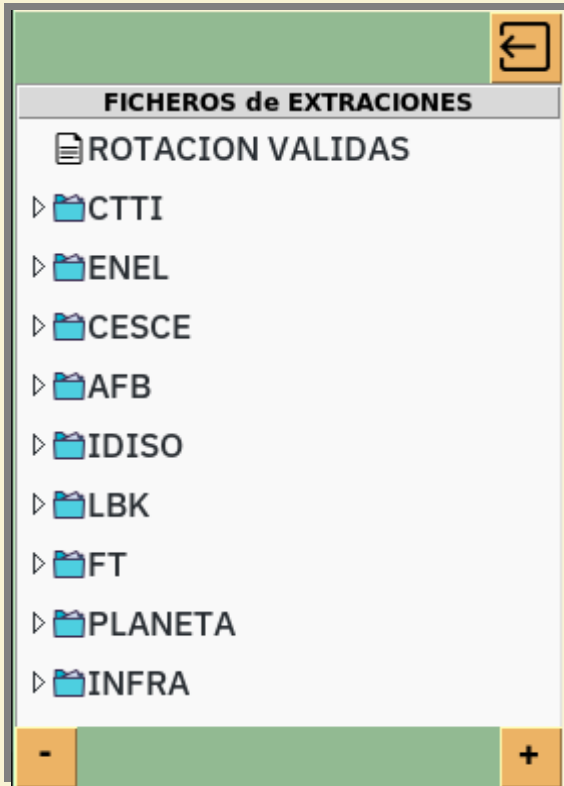
"Restrict Private Keys access using "from=" parameter on Public Keys.

// Nos habla de los valores adecuados que debe tener un FROM=

ÁREA DE EXTRACCIONES

Se compone de...


- Panel de fichero.
- Editor de texto.



ÁREA DE EXTRACCIONES,

Panel de ficheros.

Este panel de archivos, carga desde la carpeta ../extracion/, todos los archivos y carpetas que están distribuidos por clientes.

Tiene un botón para poder ocultar el panel y mostrar el panel. 

También un par de botones para hacerlo mas grande o mas pequeño:



La función del panel de archivos de extracción, es mostrar por cada cliente, un fichero TXT, donde esta distribuido por tipo de política, ya sea OS, SSH, SUDO, por plantilla y numero de preguntas “PREG” y cada distribución de politica, tiene sus respectivos modulos, con las descripción del modulo y los comandos a ejecutar, dependiendo si el resultado es positivo o negativo, respondemos con YES, NO o N/A.

ÁREA DE EXTRACCIONES

Editor de texto..

El área de texto o editor de texto, es similar a lo que ya venimos viendo un editor de texto, con sus funciones de buscar, copiar, pegar, etc etc.

En esta área de texto, nos mostrara el fichero de extracción que hayamos seleccionado desde el panel de fichero de extracción, desde esta área podremos mostrar un menú contextual



| | |
|------------------|--------|
| Buscar | Ctrl+F |
| Copiar | Ctrl+C |
| Seleccionar todo | Ctrl+A |
| Limpiar Búsqueda | Ctrl+X |
| Ocultar Panel | Ctrl+L |
| Mostrar Panel | Ctrl+L |
| Cerrar pestaña | |

- Buscar, muestra el panel de buscar, ya sea por modulo o palabras, nos indica el resultado y sus coincidencias o si no existen datos.
- Mostrar o ocultar panel.
- Limpiar búsqueda
- Seleccionar todo.
- Cerrar pestaña de extracción

La función del editor de texto, mantener en un solo lugar, todos los TXT que se vayan generando con la información, comandos de las distintas TECH SPEC para cada cliente y por politica.

ÁREA DE DESVIACIÓN

Archivo Editar Ayuda

Workspace

DESVIACIONES : INFRA

+

<

>

≡

CLIENTE / MODULO

INFRA

AD.1.1.1.2 Password Requirements

AD.1.1.13.1.0 Password Requirements

AD.1.1.3.2 Password Requirements

AD.1.8.12.6 Protecting Resources - OSRs

AD.1.8.12.7 Protecting Resources - OSRs

AD.1.8.22.2 Protecting Resources - OSRs

AD.1.8.7.2 Protecting Resources - OSRs

AD.1.9.1.3 Protecting Resources - User Resource

AD.1.9.1.4 Protecting Resources - User Resource

AV.1.1.6 Password Requirements

AV.1.1.7 Password Requirements

AV.1.2.4 Logging

AV.1.7.2.1 Identify and Authenticate Users

AV.2.1.1.2 Encryption

AV.2.1.1.3 Encryption

Linux

AD.1.1.1.2 Password Requirements

Account \$account has invalid Password Max Age setting of 99999 should be set to Customer Required Setting: 90. More secure value can be set.

Account

Para aplicar un correcto MAXAGE, hay que tener en cuenta el tipo de cuenta que se...

BACKUP

EDITAR / EVIDENCIA

EDITAR

Cambiar MAXAGE a 90

REFRESCAR

EVIDENCIA

clear

date

hostname

...

ÁREA DE DESVIACIÓN

El área de desviación, su funciones son aportar información, instrucciones, facilitar el manejo de la información, en esta área que se divide en 2 partes, parte izquierda, (cliente – modulo) y la parte de la derecha, (instrucciones y comandos).

The screenshot displays the 'ÁREA DE DESVIACIÓN' interface, which is divided into three main sections:

- CLIENTE / MODULO:** This panel on the left shows a list of modules under the 'INFRA' category. The selected module is 'AD.1.1.1.2 Password Requirements'. Other visible modules include 'AD.1.1.13.1.0 Password Requirements', 'AD.1.1.3.2 Password Requirements', 'AD.1.8.12.6 Protecting Resources - OSRs', 'AD.1.8.12.7 Protecting Resources - OSRs', 'AD.1.8.22.2 Protecting Resources - OSRs', 'AD.1.8.7.2 Protecting Resources - OSRs', 'AD.1.9.1.3 Protecting Resources - User Resc', 'AD.1.9.1.4 Protecting Resources - User Resc', 'AV.1.1.6 Password Requirements', 'AV.1.1.7 Password Requirements', 'AV.1.2.4 Logging', 'AV.1.7.2.1 Identify and Authenticate Users', 'AV.2.1.1.2 Encryption', 'AV.2.1.1.3 Encryption', 'BV.1.2.1 Logging', 'Business Use Notice/Business Use Notice R', 'Business Use Notice/PrintMotd Restriction', 'E.1.2.5.1 Logging', 'E.1.2.5.3 Logging', and 'E.1.5.18.0 Network Settings'.
- Linux:** This central panel displays the 'AD.1.1.1.2 Password Requirements' configuration. It shows a message: 'Account \$account has invalid Password Max Age setting of 99999 should be set to Custom Required Setting: 90. More secure value can be set.' Below this, there is a 'Account' button and a text area containing the instruction: '## Para aplicar un correcto MAXAGE, hay que tener en cuenta el tipo de cuenta que es: // Ya sea tipo /C/F/S/.'.
- EDITAR / EVIDENCIA:** This panel on the right is used for editing and viewing evidence. It includes an 'EDITAR' button, a 'REFRESCAR' button, and an 'EVIDENCIA' section. The 'EVIDENCIA' section displays a list of commands: 'clear', 'date', 'hostname', 'chage -l \$account', and 'cat /etc/passwd | grep -i \$account'.

ÁREA DE DESVIACIÓN

En la parte de (Cliente – Modulo), tenemos un menú con la lista de CLIENTES y un panel donde nos muestra todos los módulos que tengamos de dicho cliente, además de un buscar de módulos, estos módulos se guardan en ficheros JSON y se distribuyen por clave : valor.

En la parte de (Instrucciones – Comandos), se dividen en 5 partes:

- **Comprobación**: Instrucciones previas a cualquier modificación en el servidor.
- **Copia**: Crear copias de seguridad de los ficheros a editar.
- **Editar**: Instrucciones de como corregir el desvió
- **Refrescar**: Si hay necesidad de reiniciar un servicio, nunca un reset al servidor.
- **Evidencia** : Obtener el resultado de lo corregido.

Cada parte, contiene sus instrucciones y comandos a ejecutar, los comandos resaltan por su color rojizo.

ÁREA DE DESVIACIÓN

Ademas de tener varios botones como:

- **Riesgos e Impactos** : Abre un Calc, Excel con los riesgos e impactos.



- **Recortar texto**: Abre un script de bash, que recorta texto, el texto es el que nos viene en la descripción del modulo : **Password Requirements/Password MAX Age /etc/shadow, Password Requirements/Password MIN Age Shadow.**



- **Expandir ventana**: Cada cuadro de texto, tiene un botón de expandir, este botón abre ese cuadro de texto y lo representa en una modalidad mas grande y así se pueda leer mejor.



- **Botón de captura de pantalla**: Este botón, su función es mostrarnos un puntero en forma de +, y si seleccionamos el aérea nos captura esa aérea y os guarda una imagen .png, en ../imagenes/, esto lo usamos para sacar una evidencia de la configuración en el servidor.



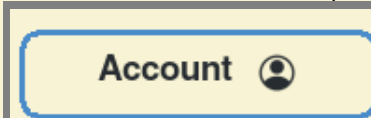
- **Botón copiar**: Este botón, solo esta en algunas partes, como en refrescar y evidencia, nos copiara todo el contenido de cada cuadro de texto.



ÁREA DE DESVIACIÓN

Existen módulos, que contienen botones extras que obtienen datos de ../file/.

Estos botones, muestran una ventana, donde obtienen datos e información, de la cuenta, el owner, el grupo al que pertenece, si tiene un riesgo, servidores, o si se se puede corregir, los datos son los mismo para cada botón, lo que cambia es el objeto, por ejemplo si es account, muestra la cuenta, si es permisión muestra el el fichero o directorio, botón se presenta de esta forma



Existen actualmente 6, botones esto se puede configurar de acuerdo a las necesidades.

- Botón ACCOUNT:
- Botón SERVICE:
- Botón PERMISSIONS:
- Botón COMMAND:
- Botón AUTHORIZED:
- Botón ID RSA:

La funciona es poder tener una base de datos, de las diferentes cuentas, y a la hora de realizar el análisis, saber si esa cuenta, fichero, servicio, se puede modificar en un servidor o varios, de esta manera agiliza la forma de trabajar, ya que no se tendrá que volver a preguntar por esa cuenta.

ÁREA DE DESVIACIÓN

Ventana expandida...

COMPROBACION

Account 



```
+-----+
## Para aplicar un correcto MAXAGE, hay que tener en cuenta el tipo de cuenta que es:

// Ya sea tipo /C/F/S/.

+-----+

+-----+
## Si es de tipo /C/, --> se pasa a excepcionar con RISK e IMPACT.

// NOTA: (Revisar el fichero de RISK e IMPACT)

+-----+

+-----+
## Si es de tipo /F/ --> se cambia a 90 dias, ejemplo de cuentas aplicable MAXAGE : root, emer,
cyberark.

## Dependiendo el cliente, alguna cuentas de TIPO F, se exepcionan con RISK e IMPACT, si fuera el
caso se debe hablar con el owner de la cuenta, y que nos indique un RISK e IMPACT, o del contrario
si se puede aplicar MAXAGE.
```

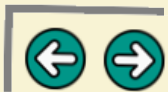
ÁREA DE DESVIACIÓN

Ventana EXPANDIDA...

Esta ventana, es la versión extendida de cada cuadro de texto de las diferentes partes de (Instrucciones – Comandos), la idea es mantener la misma información, pero en un formato mas grande y que solo sea para esa área, si por ejemplo expandes COMPROBACIÓN, mostrar las instrucciones de comprobación, si expandes EDITAR, las instrucciones de editar, etc etc.

En esta ventana, también tenemos los diferentes botones, de copiar, capturar pantalla, ACCOUNT, SERVICE, etc etc.

Añadiendo 2 botones que nos sirven para navegar entre ventanas, por ejemplo si estamos en la ventana COMPROBACIÓN, al darle a siguiente (forward →), nos llevara a la ventana de BACKUP, si estas en BACKUP, nos llevara a EDITAR y asi, lo mismo al retroceder (← back), si estas en EVIDENCIA, te lleva a comprobación.



Eso si la navegación es solo en CUADROS DE TEXTOS que **no estén VACÍOS**, si por alguna razón un cuadro de texto no contiene datos, estos botones de navegación no mostraran nada y pasaran a la siguiente ventana, por ejemplo si en BACKUP no hay datos y estamos en COMPROBACIÓN, paramos directamente a EDITAR

El Boton de expandir, se remplaza por el BOTON de REDUCIR.



ÁREA DE DESVIACIÓN

Ventana MÓDULOS..

DATOS

| NAME | OWNER | TIPO | OWNER GROUP | CODE |
|----------|----------|------|-------------|-------|
| TESAN | TESAN | F | *EPDSAN | 2-DOC |
| sklmdb40 | sklmdb40 | S | es_sd04 | 1-OK |

OTROS DATOS

SERVER

ALL Server

RISK

The non-ability to access the Storage, Special, Emte, Hyperscale Manager software process startup console

S.O : Linux

JUAN JOSE ROMERA DE F

IMPACT

Not posibilidadde manage A9K and TPC cabins from multiple customers. Degradation of the service in case of high

COMENTARIO

ÁREA DE DESVIACIÓN

Ventana MÓDULOS..

En ESTA VENTANA, muestra la información de los datos guardados de algunas cuentas, ficheros, directorios, claves privadas, claves publicas, comandos de sudo, servicios, esto con el FIN de mantener los datos en una mismo lugar, y así cada vez que tengamos nuevas desviaciones de servidores, poder comprobar si estos datos se aplican a están maquinas o si en su caso están excepcionadas, los datos que se guardan deben ser previamente analizados y comprobados con su owner, se guardan datos como, objeto o name, owner, tipo de CUENTA, grupo, y CODIFICACIÓN – code, esta codificación es la que aplicación a las issues, 1, 2 o 3, 1-OK, se va a corregir, 2-DOC se va a excepcionar, 3-OK falso positivo.

También guardados, los servidores donde solo se puede corregir o donde se excepcionan, depende la situación

Mostramos RIESGOS e IMPACTOS para poder excepcionar.

Lista de nombres de los técnicos o owner de la cuenta.

Comentario / Variable, donde se da información de algún dato si es necesario.

Coming soon: Version 3.0

- **Preferencias.**

En este modo, se implementara la posibilidad de que el usuario pueda configurar el tipo de letra, el tamaño, el color de letra o el color de ventanas y el color fondo de la APP, la pueda personalizar a su gusto

- **Modo DARK**

En este modo se implementa el << DARK MODE >>, y asi al usuario final pueda utilizarlo en iluminaciones bajas.

Jose Alvaro Cedeño Panchana