Plan de Recuperación ante Desastres

COPEC

[28/11/2023]



Integrantes :

* Fabián Muñoz
* Gabriel Soto
* Matias Perez

Asignatura :

* Seguridad en Sistemas Computacionales 021D
* Profesor Daniel Alonso Montero.

**Control de Documento**

**Preparación**

|  |  |  |
| --- | --- | --- |
| **Acción** | **Nombre** | **Fecha** |
| Preparación entorno de prueba y creación de base de datos con respaldo. | Inicio Plan de recuperación ante Desastres | 28/11/2023 |

**Versión**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versión** | **Fecha emisión** | **Cambios realizados** | **Páginas afectadas** | **Observaciones** |
| 1.0 | 28/11/2023 | TODO EL DOCUMENTO | TODAS LAS PÁGINAS |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Lista de Distribución**

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Organización** | **Cargo** |
| Gabriel Soto | Duoc UC | Operador de servidores y Database Administrator Copec |
| Matías Pérez | Duoc UC | Jefe de seguridad de la desarrollo y información Copec |
| Fabián Muñoz | Duoc UC | Analista de riesgos y jefe de equipo TI Copec |
|  |  |  |

Tabla de contenido

1. [**INTRODUCCIÓN 4**](#_heading=h.30j0zll)
   1. [Propósito 4](#_heading=h.1fob9te)
   2. [Alcance 4](#_heading=h.3znysh7)
   3. [Definiciones, Acrónimos y Abreviaturas 4](#_heading=h.2et92p0)
   4. [Referencias 4](#_heading=h.tyjcwt)
   5. [Descripción general del documento 4](#_heading=h.3dy6vkm)
2. [**PARTICIPANTES 5**](#_heading=h.1t3h5sf)
3. [**IDENTIFICACIÓN, ANÁLISIS Y PRIORIZACIÓN DE PROCESOS Y SERVICIOS CRÍTICOS TI QUE FORMAN PARTE DEL ALCANCE 6**](#_heading=h.4d34og8)
   1. [Procesos de negocio críticos y los servicios/aplicaciones TI que los soportan 6](#_heading=h.2s8eyo1)
   2. [Identificación de Dependencias de los Servicios TI 6](#_heading=h.17dp8vu)
   3. [Documentación de arquitectura de sistemas y dependencias 6](#_heading=h.3rdcrjn)
   4. [Tiempos y puntos de recuperación requeridos y factibles para sistemas y dependencias 7](#_heading=h.26in1rg)
4. [**ESTRATEGIAS DE RECUPERACIÓN 8**](#_heading=h.lnxbz9)
5. [**PROCEDIMIENTO DE ALERTA, ESCALAMIENTO, ACTIVACIÓN Y GOBIERNO DE LA RECUPERACIÓN TI 9**](#_heading=h.35nkun2)
   1. [Diagramas de Flujo 9](#_heading=h.1ksv4uv)
   2. [Descripción de equipos y roles 9](#_heading=h.44sinio)
   3. [Descripción resumida del flujo de escalamiento 9](#_heading=h.2jxsxqh)
6. [**PROCEDIMIENTOS DE CONTINGENCIA Y RECUPERACIÓN 10**](#_heading=h.z337ya)
   1. [Procedimiento de contingencia y recuperación para <nombre sistema/dependencia> 10](#_heading=h.3j2qqm3)
      1. [Objetivo 10](#_heading=h.1y810tw)
      2. [Alcance 10](#_heading=h.4i7ojhp)
      3. [Procedimientos relacionados 10](#_heading=h.2xcytpi)
      4. [Desarrollo del procedimiento 10](#_heading=h.1ci93xb)
      5. [Detalle de las tareas 11](#_heading=h.3whwml4)
7. [**ANEXOS 12**](#_heading=h.2bn6wsx)
   1. [Nómina de personal crítico con datos de contacto y reemplazantes 12](#_heading=h.qsh70q)
   2. [Nómina de proveedores críticos con datos de contacto 12](#_heading=h.3as4poj)

# Introducción

Este documento presenta el "Plan de Recuperación ante Desastres" de COPEC, centrado en salvaguardar la integridad y operatividad de su base de datos principal. Diseñado para abordar amenazas que puedan afectar los servicios críticos de Tecnologías de la Información, el plan establece procedimientos detallados y roles específicos para una recuperación rápida. Con un enfoque proactivo en la prevención, detección y mitigación de riesgos, la participación de un equipo multidisciplinario garantiza la preparación ante escenarios diversos. Este plan refleja el compromiso de COPEC con la excelencia en la gestión de crisis, la protección de datos sensibles y la continuidad operativa frente a eventos inesperados.

## Propósito

El propósito del documento es informar acerca del qué hacer y cómo restaurar la base de datos principal del sistema de Copec, dando a mostrar quienes deben participar y bajo qué circunstancias se debe aplicar

## Alcance

## Este plan aborda la recuperación de la base de datos y procesos críticos, considerando eventos como pérdida de datos, intrusiones, fallos de hardware y desastres naturales que podrían afectar las operaciones de las empresas Copec. El objetivo principal es minimizar la pérdida de datos. Este plan se aplica a todos los niveles de la organización, desde el personal de la base de datos hasta los responsables de decisiones estratégicas. La implementación y revisión periódica son fundamentales para garantizar su eficacia y adaptación a cambios en amenazas y tecnologías. En caso de desastre, se destaca la importancia de recuperar la información desde copias de seguridad para mantener la integridad y continuidad de los servicios críticos

## Definiciones, Acrónimos y Abreviaturas

* BD: Base de datos
* DB: Base de datos
* BBDD: Base de datos
* NVM: Node version manager
* IP: Protocolo de internet
* SCRIPT: Serie de instrucciones simples para un computador para que ejecute ciertas acciones, tareas o cálculos
* CPU: Unidad de procesamiento central
* RAM: Memoria de acceso aleatorio
* UEFI: Interfaz de Firmware Extensible Unificada
* TI: Tecnologías de la información
* RPO: Retorno punto objetivo
* RTO: Retorno tiempo objetivo
* SSH: Secure shell
* SH: Extensión de script para lenguajes de programación bash
* SQL: Lenguaje de consulta estructurado
* BKP: Respaldo
* Mirror: Servidor alterno de un servicio o página

## Referencias

* [César Valdes | LinkedIn](https://cl.linkedin.com/in/c%C3%A9sar-valdes-3488985)
* [César Papa Valdes email address & phone number | COPEC S.A. Chief Technology Officer contact information - RocketReach](https://rocketreach.co/cesar-papa-valdes-email_28617757)
* [COPEC S.A. Management Team | Org Chart (rocketreach.co)](https://rocketreach.co/copec-sa-management_b5c4309ef42e0d99)
* [Raul Ponte - Gestor de Servicios Networking - COPEC S.A. | LinkedIn](https://cl.linkedin.com/in/raulponte3)
* [Installing Debian via the Internet](https://www.debian.org/distrib/netinst)
* <https://saimei.ftp.acc.umu.se/debian-cd/current/amd64/iso-cd/debian-12.2.0-amd64-netinst.iso>
* [AMD EPYC™ 9754 | AMD](https://www.amd.com/es/products/cpu/amd-epyc-9754)
* [Hoja de datos de precio de HP/HPE 745813-B21 (itprice.com)](https://itprice.com/es/hp/745813-b21.html)
* [PROVANTAGE: Lenovo 7XB7A00051 4TB ThinkSystem 3.5" SATA 7.2K 6GB Hot Swap 512N Hard Disk Drive](https://www.provantage.com/lenovo-7xb7a00051~7IBMJ130.htm)
* [MZ73-LM1 (rev. 1.0) | Server Motherboard - GIGABYTE Czech Republic](https://www.gigabyte.com/cz/Enterprise/Server-Motherboard/MZ73-LM1-rev-10)
* [Descripción general - Copec RI (empresascopec.cl)](https://investor.empresascopec.cl/gobierno-corporativo/descripcion-general/)
* <https://www.trusttech.cl/docs/nch.27001.pdf/> - ISO 27001 NORMA CHILENA

## Descripción general del documento

El "Plan de Recuperación ante Desastres" de COPEC detalla de manera exhaustiva los procedimientos y estrategias diseñados para restablecer la integridad de la base de datos principal del sistema en situaciones críticas. Este plan abarca la identificación meticulosa de procesos críticos, la implementación de estrategias específicas de recuperación, la ejecución de procedimientos de alerta y la asignación de roles definidos a los equipos involucrados en la recuperación.

Un componente destacado del plan es la inclusión de un script automatizado destinado a agilizar la recuperación de la base de datos, respaldado por tiempos estimados que proporcionan una guía clara para la gestión del proceso de recuperación. Además, el documento aborda la contingencia frente a diversos tipos de desastres, como incendios o hackeos, y presenta una visión completa de la estructura organizativa y las funciones asignadas a los equipos encargados de la seguridad y el mantenimiento

# Participantes

Fabián Muñoz: Analista de riesgos y jefe de equipo TI Copec

Matias Perez: jefe de seguridad de la desarrollo e información Copec

Gabriel Soto: Operador de servidores y Database Administrator Copec

César Papa Valdez: CTO Copec

Ricardo Vilches Adasme: Gestor de Servicios Networking Copec

Hernan Villagran Tapia: CISO COPE

# Identificación, análisis y priorización de procesos y servicios críticos TI que forman parte del alcance

Todos los procesos de negocios que tengan involucrados los siguientes contextos:

* Compradores
* Empleados
* Oficinas
* Órdenes
* Pagos
* Productos

Los principales procesos de negocios afectados por una caída o desaparición de la base de datos son :

**Reconocimiento de empleados en la cajas de venta Copec** :En caso de un desastre que afecte la base de datos, los empleados enfrentarán dificultades para ser identificados, lo que obstaculizara el proceso de ventas al no poder ingresar con sus credenciales, generando problemas operativos en las cajas y afectando la eficiencia del servicio al cliente.

**Reconocimiento de información de productos**: La falta de acceso a la base de datos hará imposible el reconocimiento de productos, ya que los códigos de barras no podrán cumplir su función. Esto podría resultar en interrupciones operativas, afectando la identificación precisa de productos, la facturación y la experiencia del cliente.

**Formas de Pago** : La base de datos almacena información crítica sobre las diversas formas de pago aceptadas en COPEC. Cualquier irregularidad o fallo en este sistema podría dar lugar a problemas significativos en los procesos de pago de servicios. La falta de acceso a la información pertinente podría resultar en dificultades para procesar transacciones, afectando la eficacia en el servicio y generando inconvenientes en la gestión financiera de la organización.

**Errores de Reabastecimiento locales COPEC**:La base de datos alberga información crucial sobre las necesidades de reabastecimiento de productos en las oficinas o establecimientos COPEC. Cualquier inconveniente con esta información podría desencadenar problemas significativos, potencialmente llevando a una compleja situación de desabastecimiento en los locales COPEC.

## Procesos de negocio críticos y los servicios/aplicaciones TI que los soportan

**Proceso de Ventas en Cajas COPEC:**

Servicio de Reconocimiento de Empleados en Cajas COPEC (Sistema de Identificación de Empleados).

**Gestión de Inventario y Reabastecimiento:**

Sistema de Control de Inventario COPEC.

Aplicación de Registro de Necesidades de Reabastecimiento.

**Proceso de Pago de Servicios:**

Servicio de Formas de Pago COPEC (Sistema de Gestión de Pagos).

**Identificación y Registro de Productos:**

Sistema de Reconocimiento de Información de Productos (Base de Datos de Productos y Códigos de Barras).

## Identificación de Dependencias de los Servicios TI

Las máquinas donde estará alojada nuestro servidor de base de datos tendrá ciertas características tanto de hardware como dependencias de software

* Hardware
  + CPU: x2 AMD EPYC™ 9754
  + RAM: x24 128 GB RAM DDR5 5.5@GHz
  + Almacenamiento: Crucial T700 4 TB M.2 + (Raid 5) x5 Lenovo 4 TB (7XB7A00051)) (16 TB Utilizables)
  + Fuente 900W Redundante HP 745813-B21
  + x5 Cables interfaz SATA 3
  + Placa Madre Gigabyte MZ73-LM1
  + Teclado de oficina (opcional)
  + Monitor de oficina (opcional)
* Software
  + Sistema operativo Debian 12 minified
  + Bash
  + OpenSSH
  + MySql (MariaDB)
  + MySql-dump
  + Curl y/o Wget
  + Vim y/o Nano
  + tmux
  + htop
  + (nvm node version manager) NodeJs + npm
  + Python3 + pip
  + Certificado SSL para habilitar HTTPS

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

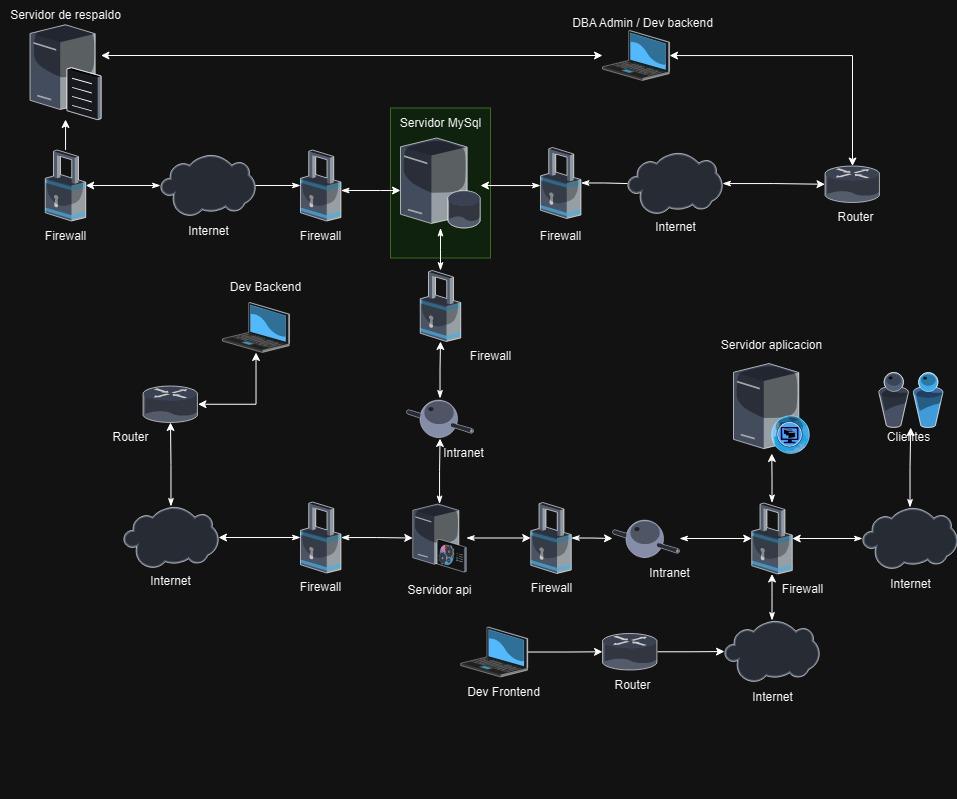
## 

## 

## 

## 

## Documentación de arquitectura de sistemas y dependencias



Todos los servidores se encontrarán en la misma subred a excepción del servidor de respaldo, este se encontraran físicamente en un lugar distinto para asegurar la integridad de los respaldos. Los equipos de desarrollo se encontrarán en una oficina externa a donde se encuentran los servidores, por lo que el sistema se estará ejecutando en un datacenter especializado en el mantenimiento de estos.

## Tiempos y puntos de recuperación requeridos y factibles para sistemas y dependencias

**RPO**

El objetivo de este punto es documentar y ejecutar la recuperación de la base de datos MySql en un servidor Linux Debian. Primero lo que debemos hacer es revisar la integridad del servidor, ya que dependiendo del desastre variará ligeramente la recuperación a nivel de hardware.

Si el servidor fue víctima de un hackeo, solamente deberemos cambiar nuestra placa madre y disco duro, adicionalmente el dispositivo de almacenamiento recibirá un tratamiento de formateo profundo. Una vez el formateo se haya completado, el dispositivo será depositado a un almacén de hardware para donaciones. Nuestra placa madre recibirá un tratamiento de reprogramación de UEFI y cambio de pila de UEFI para también ser depositada al almacén de hardware para donaciones.

En caso de que el desastre sea causado por un incendio,o lluvias extremas o un exceso de humedad el procedimiento consistirá en cambiar todo el hardware para evitar posibles fallas en producción, en el que los componentes antiguos serán llevados a su respectiva revisión técnica, en el que si los componentes pasan las pruebas especificadas en la revisión, serán depositados para el almacén de hardware para donaciones

En caso de que el hardware sea causado por un terremoto, se deberán chequear todos los dispositivos de almacenamiento en revisión técnica, verificando que su funcionamiento sea el adecuado, luego se chequeará el resto del hardware. En caso de que el hardware no pase las pruebas, se aplicará el mismo procedimiento que en casos anteriores para que el hardware que se haya podido arreglar, se pueda depositar

Una vez se hayan chequeados todos los posibles desastres y si se requiere, procederemos a la restauración del sistema de la máquina, en el que instalaremos Debian minimal, MySql + OpenSSH + tmux y luego se restaura la base de datos.

**RTO**

La recuperación tendrá una variación de tiempo según el tipo de desastre, ya dependiendo del desastre, se podrán hacer ciertas tareas en paralelo Sin embargo, estimando tiempos:

* 60 minutos- Ensamblar servidor
* 30 minutos - Instalar Debian
* 10 minutos- Instalar actualizaciones
* 1 minuto - Ejecutar script de recuperación de base de datos
* 60 minutos - Pruebas post recuperación de base de datos

TOTAL = 2 horas y 41 minutos como máximo (161 minutos) [2.68 horas] estimados para volver a operar normalmente

# Estrategias de Recuperación

Principalmente, se aplica el mismo filtro de desastres por lo que el procedimiento de instalación de hardware y sistema operativo siempre será el mismo para todos los servidores. Sin embargo al momento de instalar el software varía el procedimiento, tanto como para servidores web, de base de datos y de apis.

Principalmente nos enfocaremos en la estrategia de recuperación de base de datos. Periódicamente se ejecutará una tarea en cronjob que se encargará de subir un script que tendrá todos los comandos ejecutables + otros scripts para poder recuperar nuestros sistemas. Este script se ejecutará 2 veces al día cada 12 horas, la primera vez a las 02:00 hrs y la segunda vez a las 14:00 hrs.

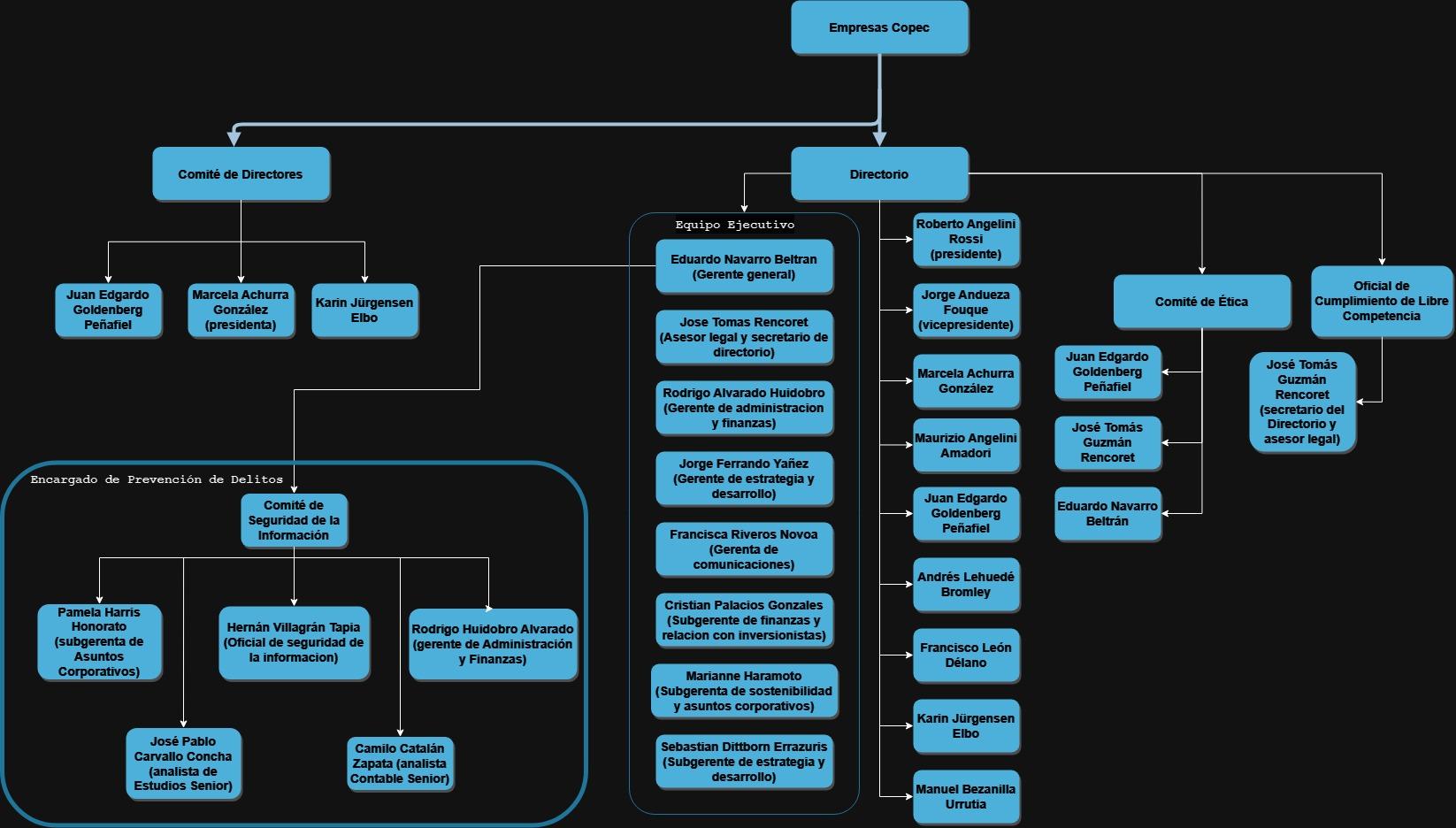
Cuando llegue el momento de restaurar el los sistemas ante un desastre, instalaremos nuestro sistema operativo y lo primero que haremos será actualizarlo, seguido de eso instalaremos tmux, wget, curl, vim, y nano, una vez instalados los programas mencionados, ejecutaremos el comando wget seguido del archivo con el script para restaurar nuestra base de datos. Todo esto al ser de manera automatizada, nos permitirá volver a nuestro funcionamiento normal de una manera rápida y eficaz

# Procedimiento de alerta, escalamiento, activación y gobierno de la recuperación TI

Según el tipo de alerta el gobierno sufrirá un cambio distinto

Mediante un sistema de Prevención y detección de intrusos se podrá activar la alerta de desastre por ataque informático, en este caso las escalas dentro del gobierno sufrirán de un cambio desde el equipo ejecutivo, en el que el CISO será el mandatario y el CEO el segundo al mando, ambos puestos trabajaran en conjunto para regular el funcionamiento de los sistemas y volver a operar con normalidad lo antes posible.

Si se activa por un incendio, lluvias extremas y humedad o terremoto se activará la alerta de desastre respectiva, en estos casos las escalas dentro del gobierno sufrirán un cambio en el que el CEO será el mandatario y el CISO el segundo al mando ambos puestos



En este caso, el podemos ver que el comité de seguridad y de la información es liderado por el CISO Hernan Villagran Tapia, por lo que si llegase a efectuarse una alerta de desastre, **todo el equipo del comité estará por sobre el equipo ejecutivo**

## 

## 

## 

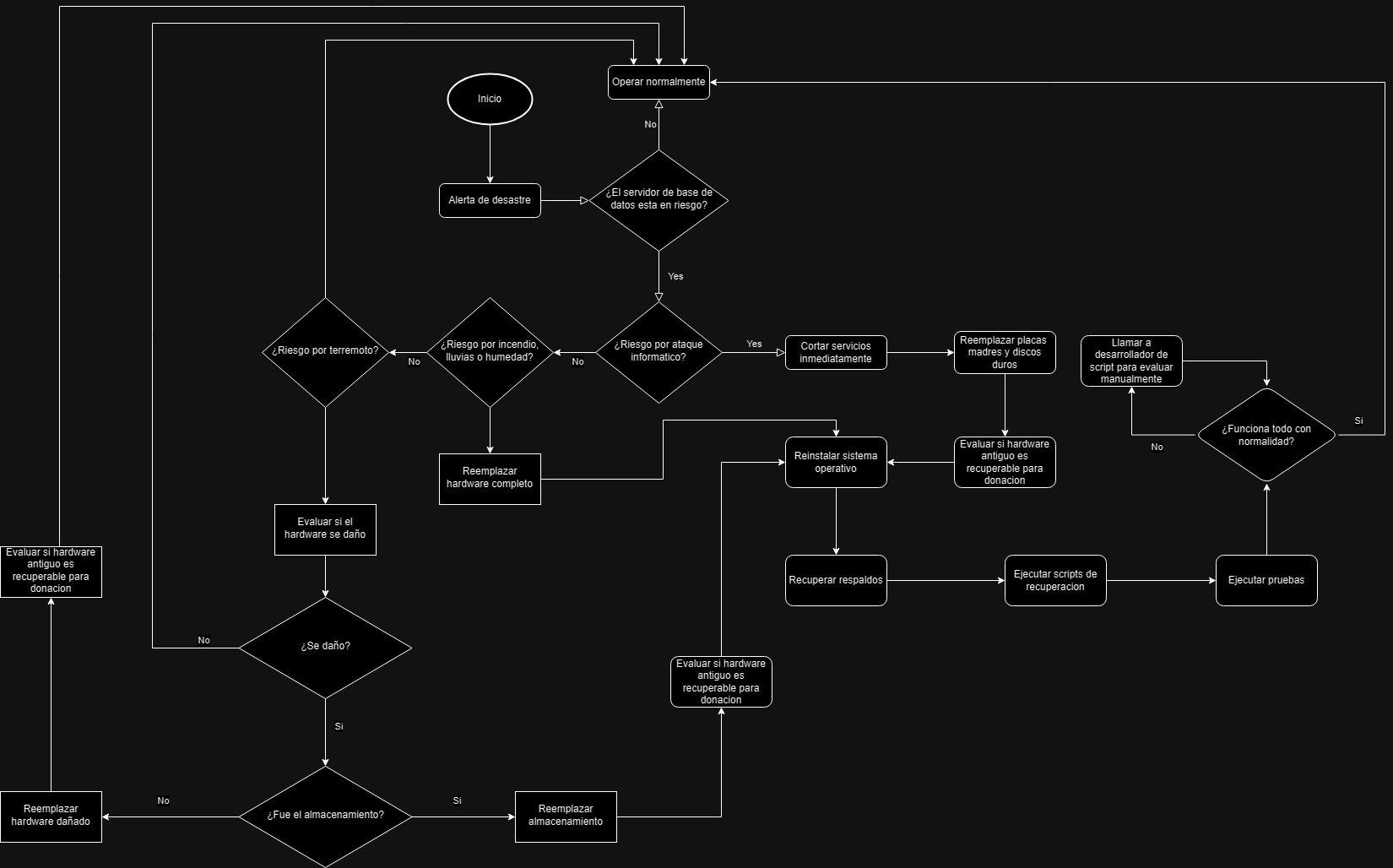
## 

## 

## 

## 

## Diagramas de Flujo



## Descripción de equipos y roles

**Equipo de Seguridad**: Este equipo está encargado de salvaguardar la seguridad de las bases de datos, así como de implementar medidas para proteger la información sensible. Sus roles incluyen la supervisión de accesos, la gestión de sistemas de vigilancia, la coordinación con autoridades locales en caso de cambios por posibles amenazas y vulnerabilidades.

**Equipo de Mantenimiento**: Este equipo se encarga de preservar la operatividad de los servidores físicos, distribuidos entre el equipo interno de COPEC y el externo que administra los servidores de nuestras instalaciones. Ambos equipos colaboran de manera coordinada para garantizar un óptimo funcionamiento.

## Descripción resumida del flujo de escalamiento

El proceso de escalonamiento se activará al entrar en el estado de alerta, dando lugar a una redistribución de roles entre el comité de seguridad de la información y el equipo directivo. Esto resultará en una disminución de la influencia y autoridad del equipo directivo en las decisiones empresariales, durante el periodo en que se mantenga el estado de alerta por desastre. Este ajuste temporal se revertirá una vez que Copec restablezca sus operaciones normales.

# Procedimientos de Contingencia y Recuperación para servidor de base de datos

## Objetivo

El objetivo de este punto es documentar y ejecutar la recuperación de la base de datos MySql en un servidor Linux Debian siguiendo los indicados en el diagrama del punto 5.1

* 1. Alcance

En caso de que el servidor fue víctima de un hackeo, solamente deberemos cambiar nuestra placa madre y disco duro, adicionalmente el dispositivo de almacenamiento recibirá un tratamiento de formateo profundo. Una vez el formateo se haya completado, el dispositivo será depositado a un almacén de hardware para donaciones. Nuestra placa madre recibirá un tratamiento de reprogramación de UEFI y cambio de pila de UEFI para también ser depositada al almacén de hardware para donaciones.

En caso de que el desastre sea causado por un incendio,o lluvias extremas o un exceso de humedad el procedimiento consistirá en cambiar todo el hardware para evitar posibles fallas en producción, en el que los componentes antiguos serán llevados a su respectiva revisión técnica, en el que si los componentes pasan las pruebas especificadas en la revisión, serán depositados para el almacén de hardware para donaciones

En caso de que el desastre sea causado por un terremoto, se deberán chequear todos los dispositivos de almacenamiento en revisión técnica, verificando que su funcionamiento sea el adecuado, luego se chequeará el resto del hardware. En caso de que el hardware no pase las pruebas, se aplicará el mismo procedimiento que en casos anteriores para que el hardware que se haya podido arreglar, se pueda depositar

* 1. Procedimientos relacionados

Debido a que la situación de desastre es considerada una situación de suma urgencia, apenas se entre en este estado lo primero que se cambiarán serán las jerarquías de gobierno entre el equipo de comité de seguridad y el equipo ejecutivo sin necesidad de un documento de por medio. Una vez el equipo ejecutivo termine su trabajo, deberán volver a sus posiciones normales ambas entidades, y ambas entidades deberán generar un reporte de que es lo que se ha hecho durante y post desastre, adicionalmente el equipo ejecutivo deberá generar un reporte de que es lo que se estuvo haciendo pre desastre en todos sus departamentos que tengan a su disposición, esto con la finalidad de poder hacer un seguimiento a que fue lo que paso en caso de que haya sido un desastre por ataque informático.

* 1. Desarrollo del procedimiento



Fase de transición a operación en contingencia (failover)

El estado de failover dará luz verde por el verde si es que es dado desde el por alguna entidad mayor Directorio, el comité de directores, El presidente del directorio o el Gerente General, Este último deberá obtener un respaldo de alguna de las entidades antes mencionadas para comenzar el failover. Sin embargo, si existe un evidente ataque informático y ninguna entidad de las tres primeras entidades se manifiesta en 1 hora el comité de seguridad tendrá total facultad de tener control por sobre el equipo ejecutivo. Si es que algún integrante del comité de seguridad llegase a forzar esta situación de manera malintencionada o de forma que perjudique a Copec, el comité de ética contará con las herramientas para poder controlar esta situación, contando con un equipo externo especializado para investigación y análisis forense.

Fase de operación en contingencia

Una vez llegado este procedimiento, se deberá determinar por qué comenzó el desastre, según el tipo de desastres se deberá actuar de manera diferente según lo indicado en el diagrama de flujo y en lo indicado en el RPO y el Alcance.

Fase de transición a operación normal o vuelta atrás (failback)

Una vez se haya logrado identificar el problema, tomar las acciones necesarias y resolver a primera vista, el comité de seguridad en conjunto con el equipo desarrollador y el DBA deberán hacer un testeo de por lo menos 1 hora en los sistemas para asegurarse de que todo está funcionando con normalidad, en estos testeos estarán incluidos los cambios de credenciales, las aperturas de puertos específicas en los servidores y el levantamiento de servicios necesarios para el funcionamiento del sistema. Una vez pasadas las todas las pruebas el equipo ejecutivo y todos sus departamentos y empleados deberán reportar que es lo que estuvieron haciendo pre-desastre, durante el desastre y post-desastre, mientras que el comité de seguridad deberá reportar las actividades hechas durante el desastre y acciones a tomar post-desastre.

* 1. Detalle de las tareas

Primero, se debe definir porque se produjo el desastre. Dependiendo que tipo de desastre sea se ejecutará cierto procedimiento en el hardware del servidor. La clasificación de las alertas de desastres están definidas en los puntos del **RPO** y **Alcances** por lo que ahora se explicará en detalle el diagrama de flujo.

**Desastre por incendio**

1. Apagar servidor, desarmarlo y llevarlo a revisión técnica
   1. Validar si es apto para donación de hardware
   2. Donarlo a alguna entidad, fundación o universidad
2. Preparar nuevamente el ambiente fisico nuevo donde se instalará el servidor con hardware totalmente nuevo
3. Armar el servidor con las especificaciones de hardware mencionadas en el punto 3.2
4. Instalar offline la distribución Debian de linux en su versión minified
5. Conectar cable lan al servidor para proporcionar internet
6. Instalar actualizaciones haciendo uso del comando:  
   $ sudo apt-get update && sudo apt-get upgrade
7. Una vez actualizado el sistema, instalar wget y curl usando el comando:  
   $ sudo apt-get install wget && curl
8. Una vez instalados estos dos programas, podemos recuperar nuestros scripts para recuperar nuestra base de datos desde nuestro servidor externo de respaldo, esto lo podremos lograr ejecutando los siguientes comando:  
   $ wget <https://cdn.discordapp.com/attachments/823996451397828678/1178486571402543144/MySqlbackup.sh>
9. Ejecutar el comando `chmod +x MySqlbackup.sh`.Este script descargado contiene el siguiente contenido:

#!/bin/bash

#

# Autor: Gabriel Soto / Estudiante ingenieria en informatica DuocUC

# 2023 - Seguridad en sistemas computacionales

#

# Este script consistira restaurar el servidor de base de datos de Copec

# ante diversos tipos de amenazas, como por ejemplo:

# - Hackeos

# - Desastres naturales

# - etc

#

# Variables globales

google="www.google.com"

intentos=3

servicio="mysql"

archivo="/etc/mysql/mariadb.conf.d/50-server.cnf"

## Colores de texto

rojo='\033[0;31m'

verde='\033[0;32m'

amarillo='\033[0;33m'

azul='\033[0;34m'

magenta='\033[0;35m'

cyan='\033[0;36m'

blanco='\033[0;37m'

## Colores de fondo

fondoRojo='\033[41m'

fondoVerde='\033[42m'

fondoAmarillo='\033[43m'

fondoAzul='\033[44m'

fondoMagenta='\033[45m'

fondoCyan='\033[46m'

fondoBlanco='\033[47m'

reset='\033[0m' # Restablecer el color

ManejarError(){

echo -e "${fondoRojo}Ocurrio un error desconocido. Deteniendo el script...${reset}"

exit 1

}

VerificarPermisos(){

if [ "$(whoami)" != "root" ]; then

echo -e "${fondoRojo}Este script debe ser ejecutado como root.${reset}"

exit 1

fi

}

VerificarConexion(){

if ping -c 1 -W 2 $google > /dev/null 2>&1; then

echo -e "${verde}Conexion a internet exitosa.${reset}"

else

echo -e "${rojo}No hay conexion a internet.${reset}"

fi

}

VerificarDistro(){

if [ -f /etc/os-release ]; then

source /etc/os-release

if [ "$ID" = "debian" ]; then

echo ""

else

echo -e "${fondoRojo}Este script solo esta hecho para funcionar en distros Debian. Deteniendo el script...${reset}"

exit 1

fi

else

echo -e "${fondoRojo}No se pudo determinar el sistema operativo. Deteniendo el script...${reset}"

fi

}

Timer(){

for ((i = 1; i <=$1; i++)); do

echo "."

sleep 1

done

}

PresionaParaSalir() {

Timer 5

clear

echo -e "${fondoVerde}Todo listo! Presiona cualquier tecla para salir${reset}"

read -n 1 -s -r -p "" # Espera a que el usuario presione una tecla

exit 1

}

main(){

trap 'ManejarError' ERR

VerificarPermisos

VerificarDistro

clear

# Haremos 3 intentos para verificar la conexion a internet

for ((i = 1; i <=$intentos; i++)); do

echo -e "Revisando conexion ($i / 3):"

VerificarConexion

break

if [ $i -lt $intentos ]; then

sleep 2 # esperar antes del proximo intento

fi

done

# Actualizamos sistema y instalamos mysql + otros recursos

echo -e "${amarillo}Actualizando sistema...${reset}"

sudo apt-get update > /dev/null 2>&1 && sudo apt-get upgrade > /dev/null 2>&1

echo -e "${verde}Listo!${reset}"

echo -e "${amarillo}Instalando MySql-server${reset}"

sudo apt-get install default-mysql-server > /dev/null 2>&1

echo -e "${verde}Listo!${reset}"

# Checkeamos si el servicio mysql esta activo, en caso de que no lo este, lo levantamos

echo -e "${amarillo}Checkeando si el servicio ${servicio} esta arriba${reset}"

if systemctl is-active --quiet $servicio; then

echo -e "${verde}El servicio ${magenta}${servicio} ${verde}está activo.${reset}"

else

echo -e "${rojo}El servicio ${magenta}${servicio} ${rojo}no está activo. ${amarillo}Activando servicio${reset}"

systemctl start mysql

echo -e "${verde}Listo!${reset}"

fi

Timer 3

clear

# Creamos nuestro usuario en la base de datos y le asignamos permisos

read -p "¿Como deberia llamarse el usuario a crear en mysql? (ENTER = 'dba'): " usuario

if [ -z "$usuario" ]; then

usuario="dba"

fi

read -s -p "¿Cual seria su clave? (ENTER = '\*\*\*\*\*\*\*\*'):" clave

if [ -z "$clave" ]; then

clave="2023duoc"

fi

echo ""

echo -e "${amarillo}Creando usuario ${magenta}'${usuario}' ${amarillo}en la base de datos...${reset}"

mysql -u root -e "CREATE USER '${usuario}'@'localhost' IDENTIFIED BY '${clave}';"

mysql -u root -e "CREATE USER '${usuario}'@'%' IDENTIFIED BY '${clave}';"

echo -e "${amarillo}Asignandole permisos...${reset}"

mysql -u root -e "GRANT ALL PRIVILEGES ON \*.\* TO '${usuario}'@'localhost';"

mysql -u root -e "GRANT ALL PRIVILEGES ON \*.\* TO '${usuario}'@'%';"

mysql -u root -e "FLUSH PRIVILEGES;"

echo -e "${verde}Listo!${reset}"

Timer 3

clear

# Recuperamos nuestro respaldo de la base de datos

echo -e "${amarillo}Recuperando base de datos del servidor de respaldo...${reset}"

## Checkeamos si existe

resultado=$(mysql -u root -e "SHOW DATABASES LIKE 'copec';" 2>/dev/null)

if [[ $resultado == \*"copec"\* ]]; then

mysql -u root -e "drop database copec;"

fi

if [ -f "./respaldobdcopec.sql" ]; then

rm ./respaldobdcopec.sql

fi

curl https://cdn.discordapp.com/attachments/823996451397828678/1177346494798508092/mysqlsampledatabase.sql --output ./respaldobdcopec.sql > /dev/null 2>&1

echo -e "${verde}Listo!${reset}"

echo -e "${amarillo}Restaurando la base de datos en el servidor...${reset}"

mysql -u root < respaldobdcopec.sql

echo -e "${verde}Listo!${reset}"

Timer 3

clear

# Editamos el archivo de configuración de mysql para permitir conexiones remotas

echo -e "${amarillo}Editando configuraciones de mysql...${reset}"

sed -i 's/bind-address[[:space:]]\*=[[:space:]]\*127.0.0.1/# bind-address = 127.0.0.1/' "$archivo"

sed -i '/# bind-address = 127.0.0.1/a bind-address = 0.0.0.0' "$archivo"

echo -e "${verde}Listo!${reset}"

echo -e "${amarillo}Reiniciando servicio mysql...${reset}"

sudo systemctl restart mysql

echo -e "${verde}Listo!${reset}"

PresionaParaSalir

}

Básicamente, este script automatiza todo el proceso de actualización de sistema, instalación de MySql, configuración para conexiones remotas de MySql, creación de usuario de MySql y aplicación de base de datos con sus respectivos registros en nuestra base de datos.

El script cuenta con entradas de usuario y contraseña para lo que es la creación de usuarios en la BD.

1. Ejecutar el comando:

sudo ./MySqlbackup.sh

1. Ejecutar las respectivas pruebas entre desarrolladores, DBA y Operadores de seguridad
2. Verificar que todo esté en orden
3. Volver al funcionamiento normal

**Desastre por lluvia, exceso de humedad o terremoto**

1. Apagar servidor, desarmarlo y llevarlo a revisión técnica
   1. Validar si hardware está en estado para volver a su funcionamiento habitual o si el hardware se ha roto pero tiene arreglo para poder donarlo
   2. Donarlo hardware arreglado a alguna entidad, fundación o universidad
   3. Volver con hardware que se validó como bueno para rearmar el servidor
2. Preparar nuevamente el ambiente fisico nuevo donde se instalará el servidor con hardware, reemplazar las piezas faltantes
3. Armar el servidor con las especificaciones de hardware mencionadas en el punto 3.1. **Si se daño algún dispositivo de almacenamiento del sistema operativo** **el procedimiento debe seguir para la reinstalación de todo el software**, caso contrario, si el dispositivo de almacenamiento está intacto el procedimiento saltaría directamente a las pruebas para volver a producción.
4. Instalar offline la distribución Debian de linux en su versión minified
5. Conectar cable lan al servidor para proporcionar internet
6. Instalar actualizaciones haciendo uso del comando:  
   $ sudo apt-get update && sudo apt-get upgrade
7. Una vez actualizado el sistema, instalar wget y curl usando el comando:  
   $ sudo apt-get install wget && curl
8. Una vez instalados estos dos programas, podemos recuperar nuestros scripts para recuperar nuestra base de datos desde nuestro servidor externo de respaldo, esto lo podremos lograr ejecutando los siguientes comando:  
   $ wget <https://cdn.discordapp.com/attachments/823996451397828678/1178486571402543144/MySqlbackup.sh>
9. Se ejecuta el comando  
   $ chmod +x ./MySqlbackup.sh && sudo ./MySqlbackup.sh

(El funcionamiento del script fue explicado en el primer desastre)

1. Ejecutar las respectivas pruebas entre desarrolladores, DBA y Operadores de seguridad
2. Verificar que todo esté en orden
3. Volver al funcionamiento normal

**Desastre por ataque informático**

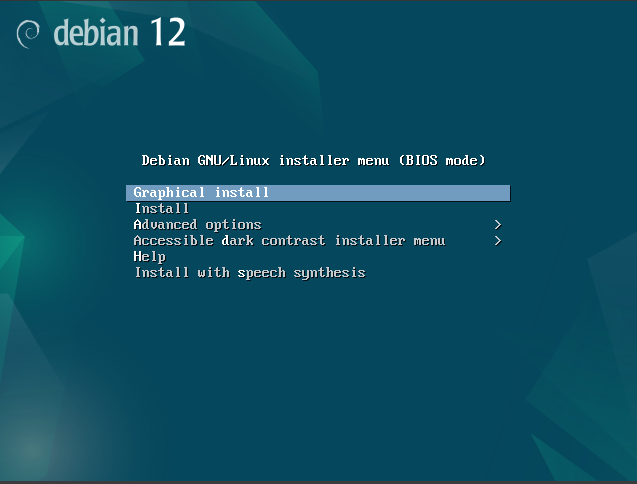
1. Apagar servidor, desarmarlo y llevarlo a revisión técnica
   1. Validar si dispositivo de almacenamiento y placa madre puede ser formateada para eliminar el posible malware.
   2. Donarlo hardware restaurado a alguna entidad, fundación o universidad
2. Preparar nuevamente el ambiente fisico nuevo donde se instalará el servidor con hardware, reemplazar las piezas faltantes
3. Armar el servidor con las especificaciones de hardware mencionadas en el punto 3.1. Instalar offline la distribución Debian de linux en su versión minified
4. Conectar cable lan al servidor para proporcionar internet
5. Instalar actualizaciones haciendo uso del comando:  
   $ sudo apt-get update && sudo apt-get upgrade
6. Una vez actualizado el sistema, instalar wget y curl usando el comando:  
   $ sudo apt-get install wget && curl
7. Una vez instalados estos dos programas, podemos recuperar nuestros scripts para recuperar nuestra base de datos desde nuestro servidor externo de respaldo, esto lo podremos lograr ejecutando los siguientes comando:  
   $ wget <https://cdn.discordapp.com/attachments/823996451397828678/1178486571402543144/MySqlbackup.sh>
8. Se ejecuta el comando  
   $ chmod +x ./MySqlbackup.sh && sudo ./MySqlbackup.sh
   1. (El funcionamiento del script fue explicado en el primer desastre)
9. Ejecutar las respectivas pruebas entre desarrolladores, DBA y Operadores de seguridad
10. Verificar que todo esté en orden
11. Volver al funcionamiento normal

**\*Recomendaciones posteriores:**

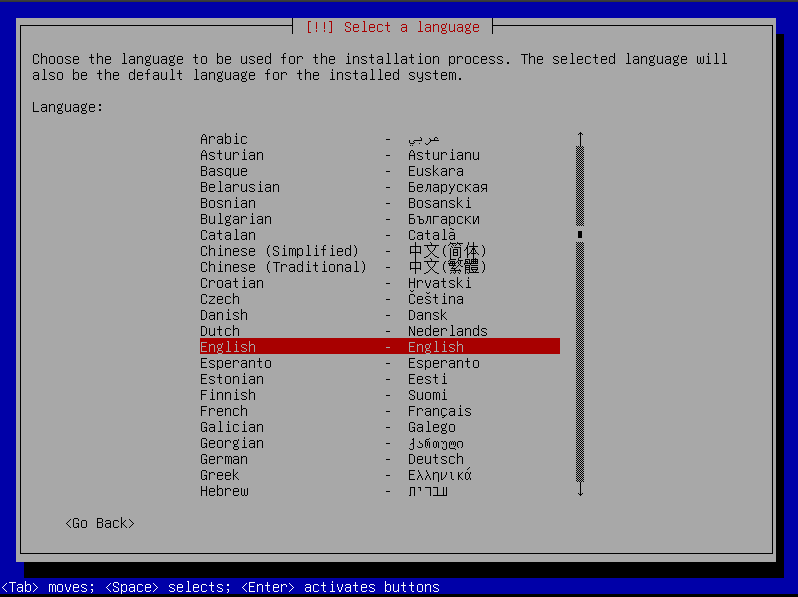
1. Aplicar hardening
2. establecer políticas para actualización de credenciales de forma semestral en la que los credenciales a usar cumplan con ciertas condiciones como por ejemplo:
   1. Que contenga por lo menos un signo
   2. Por lo menos una letra mayúscula
   3. Por lo menos 2 números en la contraseña
   4. La contraseña no puede repetirse con alguna contraseña utilizada anteriormente
   5. Mínimo 12 caracteres
3. Cerrar puertos que no están en ejecución por algún programa
4. Cambiar los puertos que usa por defecto un programa. Por ejemplo, el servicio de SSH usa el puerto 22 por defecto. Cambiarlo al puerto 254
5. Cerrar servicios que sean innecesarios para la finalidad del servidor. Si el servidor es de MySql BD, No razón alguna de tener un servicio samba arriba
6. De ser necesario, actualizar periódicamente los programas y sistemas a utilizar.
7. Establecer políticas para que Ips específicas puedan conectarse remotamente a los servidores
8. Actualizar firewall periódicamente
9. Asegurar la destrucción y quema de documentos sensibles en ambiente seguros.
10. Hacer pruebas de seguridad en la oficina semestralmente a los trabajadores
11. El sistema de respaldos a usar es Amanda, por lo que se debe configurar postrecuperacion del servidor lo antes posible (DOCUMENTACION PARA RESPALDOS DE MYSQL: https://mysqlbackup.zmanda.com/index.php/MySQL\_Backup\_and\_Recovery)

**Imágenes del procedimiento a para restauración**

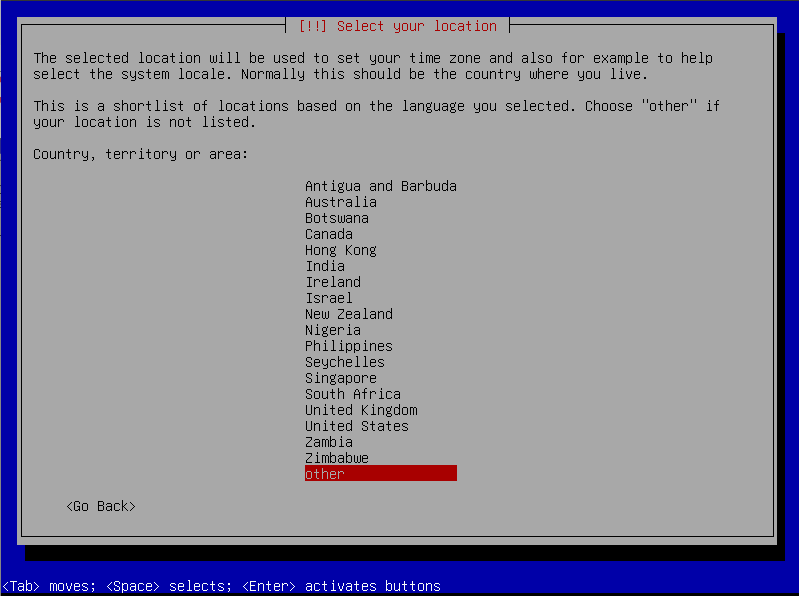
1. Booteamos el servidor desde un USB con la ISO del sistema operativo descargado, en este caso, debian 12 y seleccionamos Install

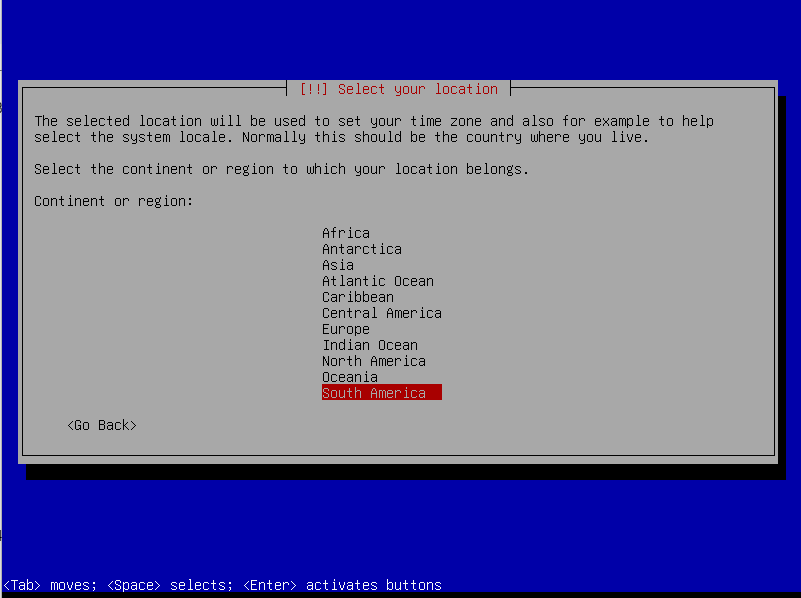
****

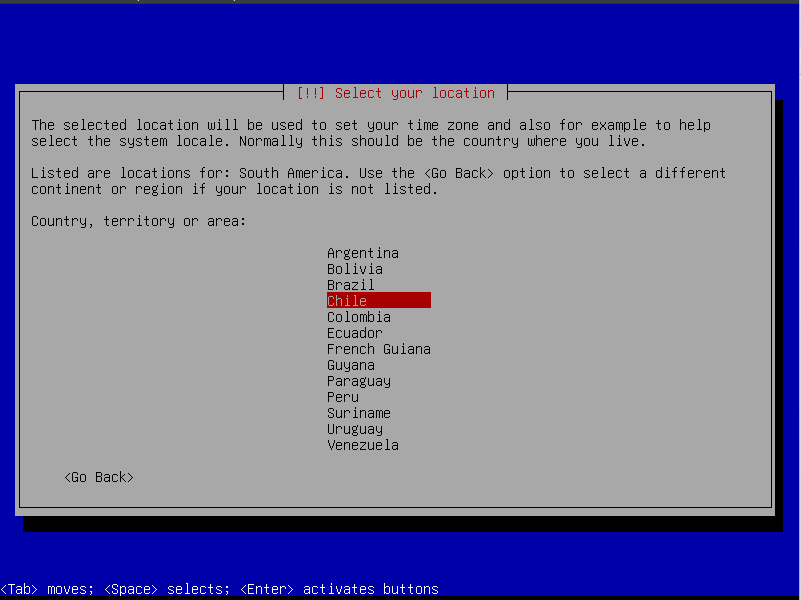
1. Elegimos el idioma que más nos acomode, en nuestro caso usaremos el inglés



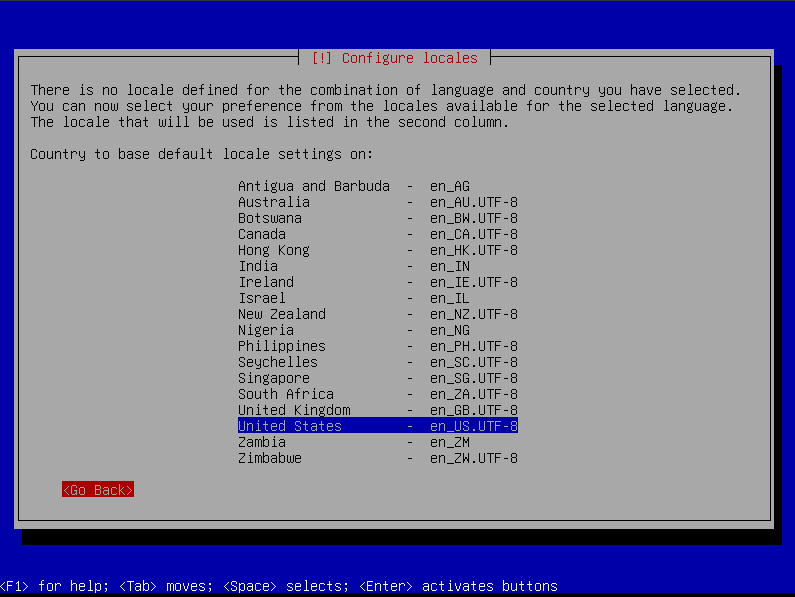
1. Como ubicación le diremos que vivimos en ‘Other’,‘South america’ y ‘Chile’’

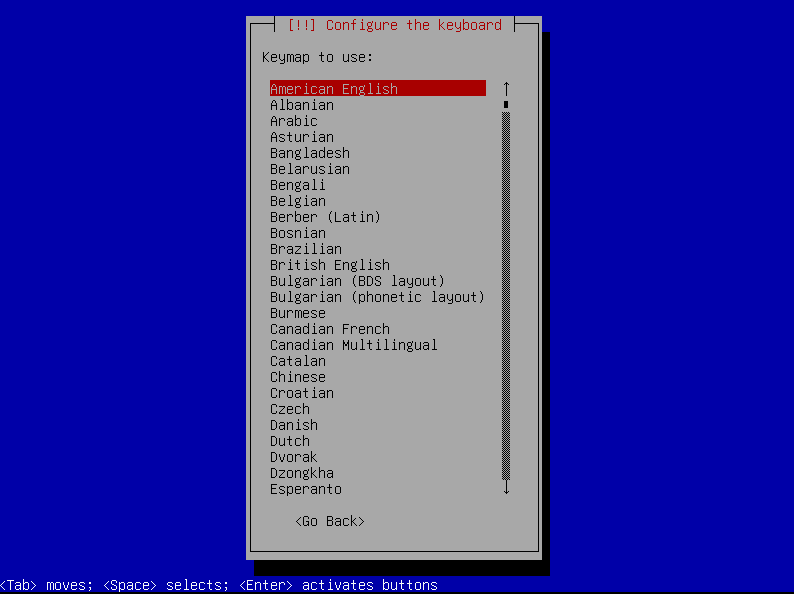






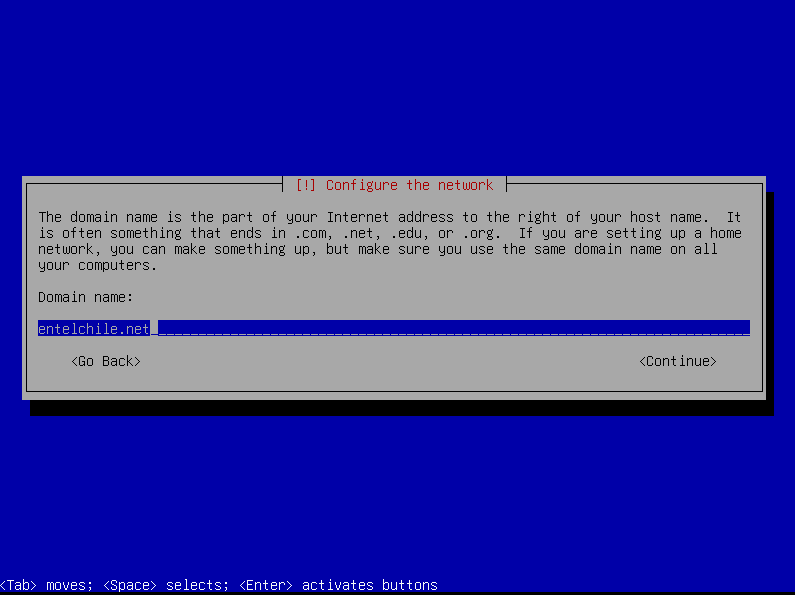
1. Luego daremos el formato de nuestro teclado. Si nuestro teclado físico tiene una Ñ lo ideal es que se seleccione el formato español en latinoamérica, sin embargo es probable que se tenga un teclado en inglés. En nuestro caso usaremos el último formato mencionado.



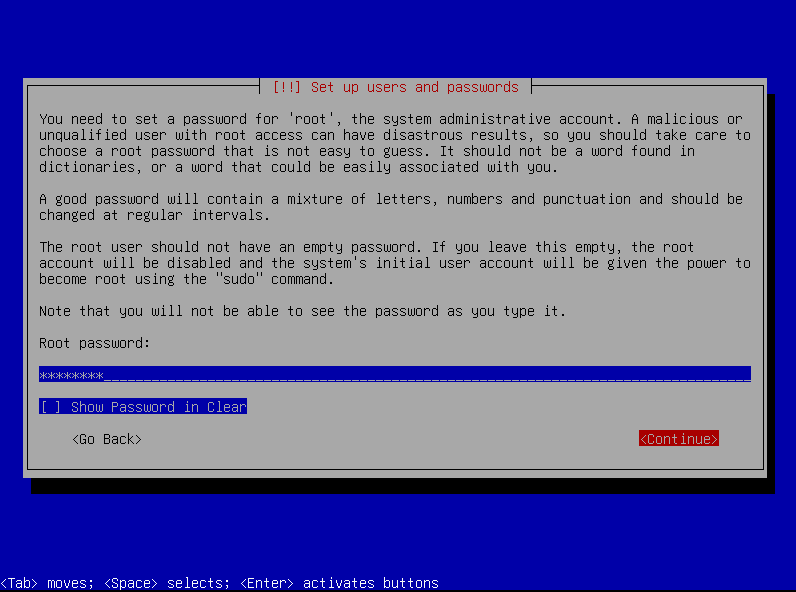


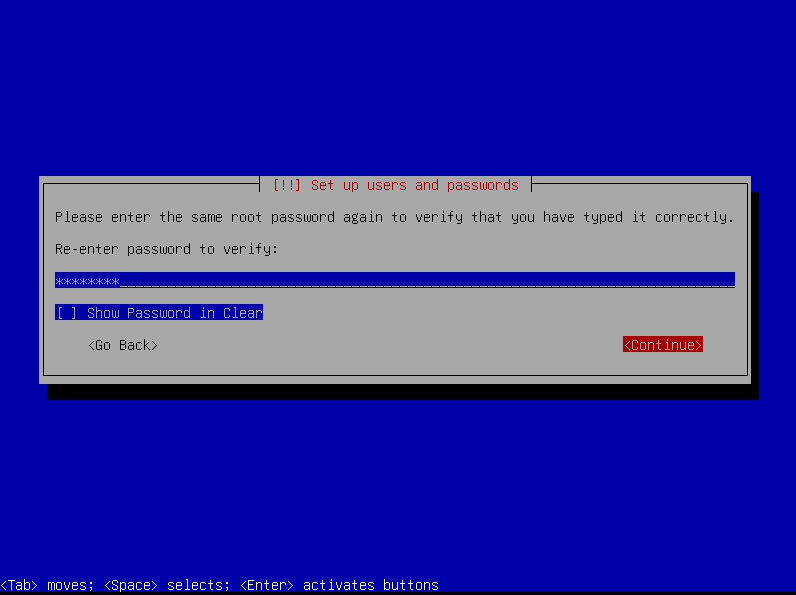
1. Nos preguntará por el nombre del host (o nombre del servidor), podemos dejar este espacio con el valor que nos da por defecto o cambiarlo



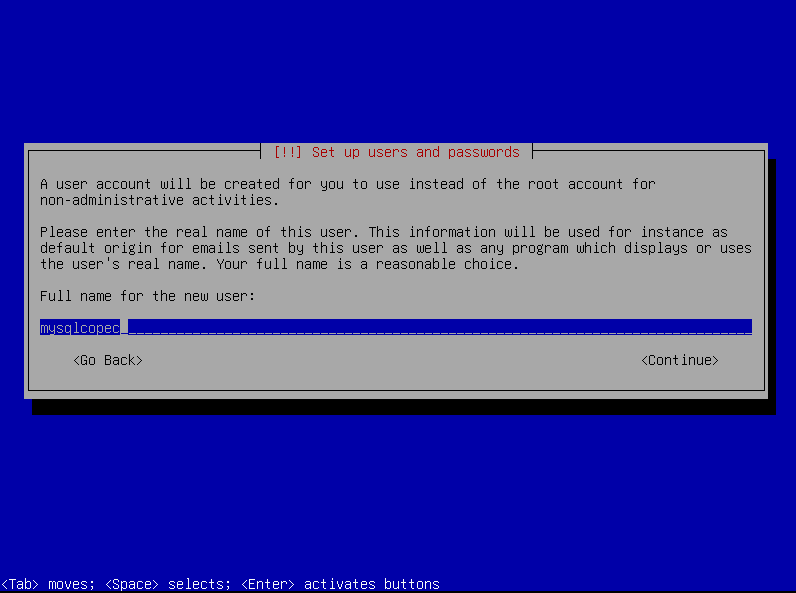


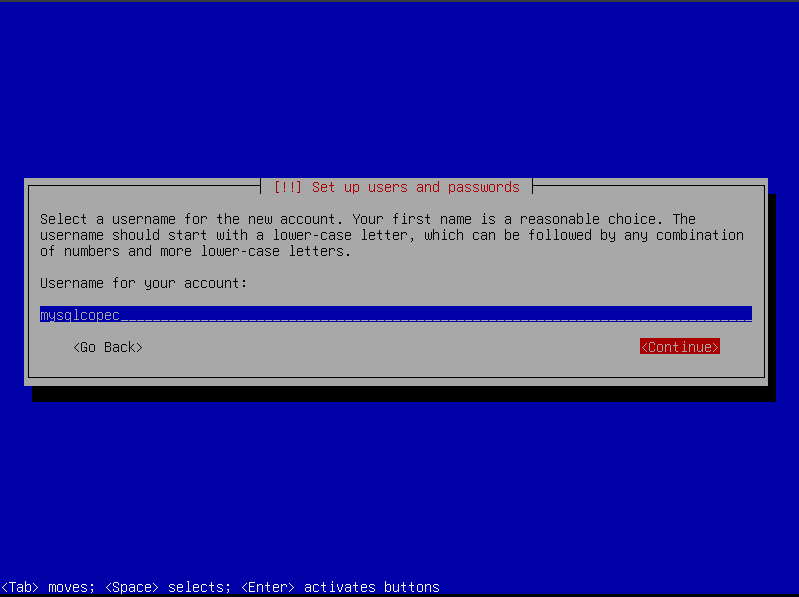
1. Una vez configurado el host, nos preguntará por la clave de nuestro usuario **root**, por ahora nuestra clave será ‘duoc2023’, luego nos pedirá nuevamente confirmar la contraseña pero se pide encarecidamente que la clave se cambie apenas se termine de configurar la máquina.

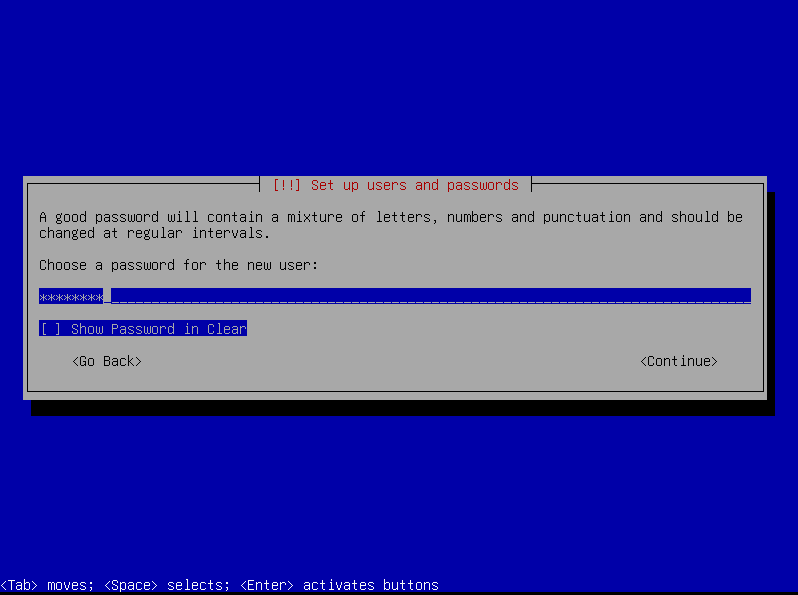




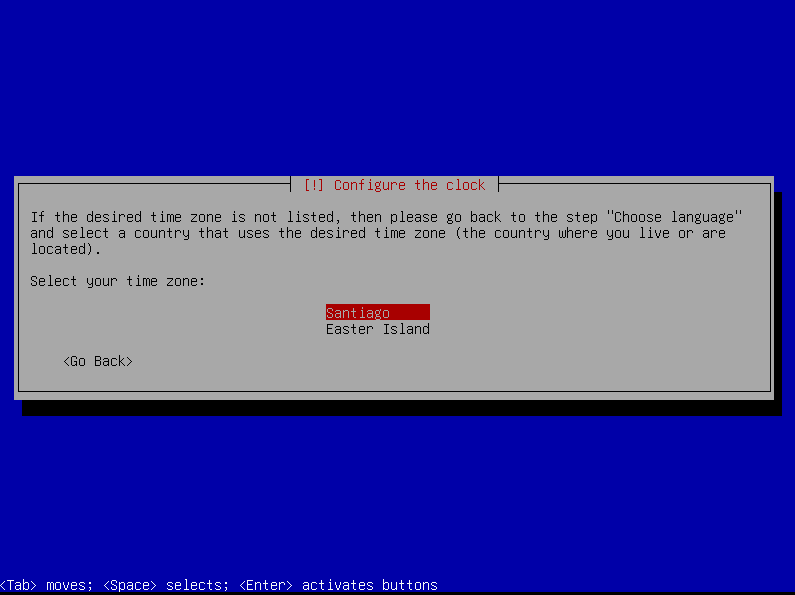
1. Ahora daremos los datos de usuario para la cuenta para usos no administrativos, el cual será ‘mysqlcopec’ y luego daremos enter nuevamente para darle los permisos de ejecución de comandos de administrador. Luego de esto, nos pedirá una clave para nuestra cuenta recien creada, la cual pondremos la misma contraseña de nuestro usuario root, la cual nos pedirá que configuremos para asegurarnos que la clave



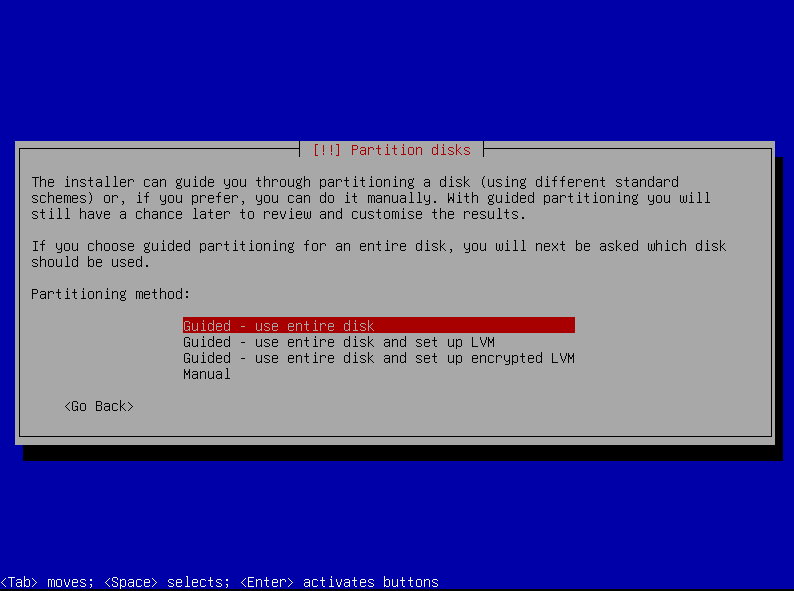


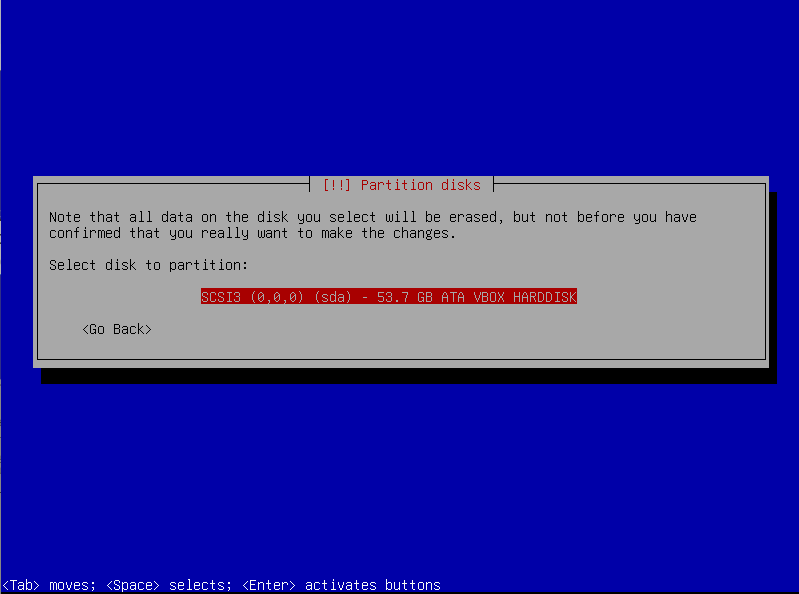


1. Configuramos nuestra zona horaria en Santiago

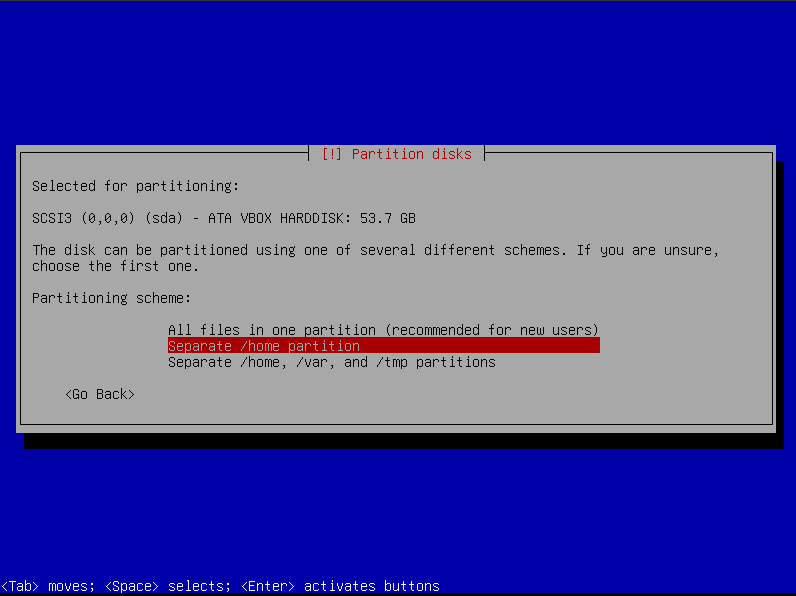


1. Particionamos el disco, usaremos la primera opción (usar el disco completo) y luego seleccionamos nuestro dispositivo de almacenamiento.

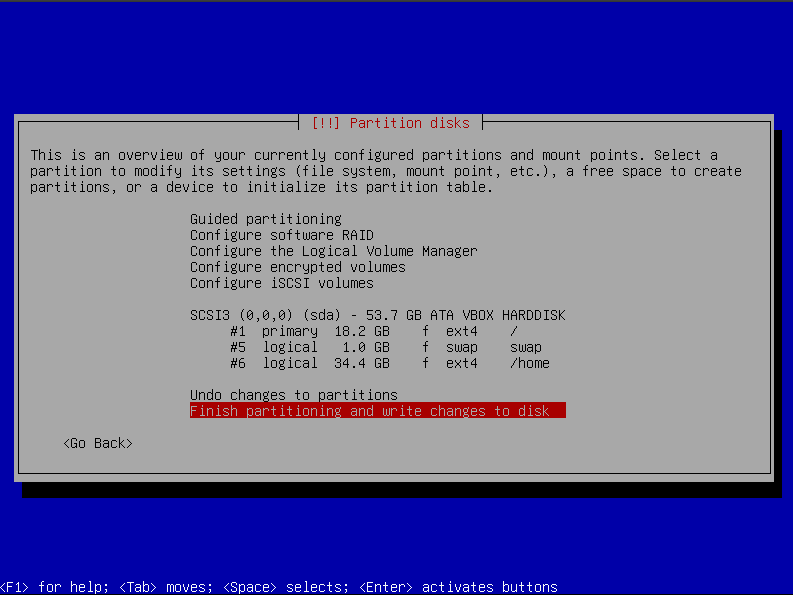




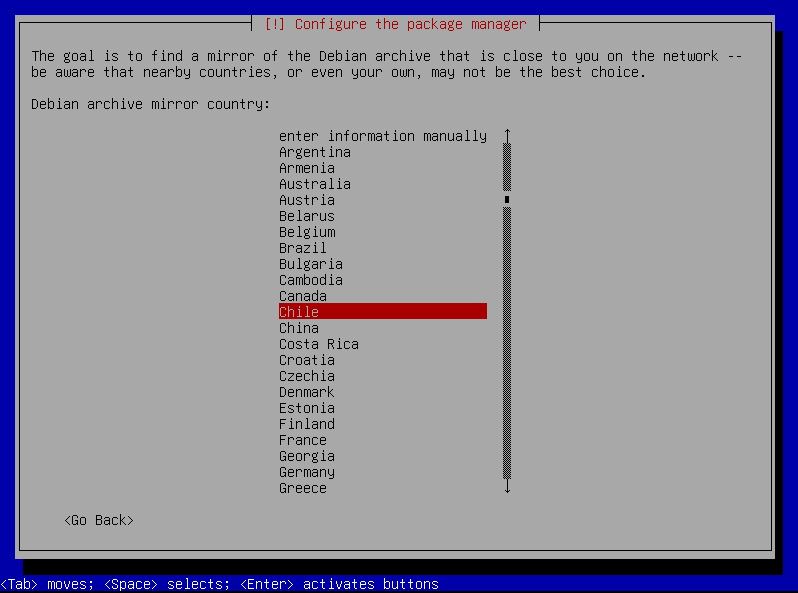
1. Usaremos la opción que nos separa la partición

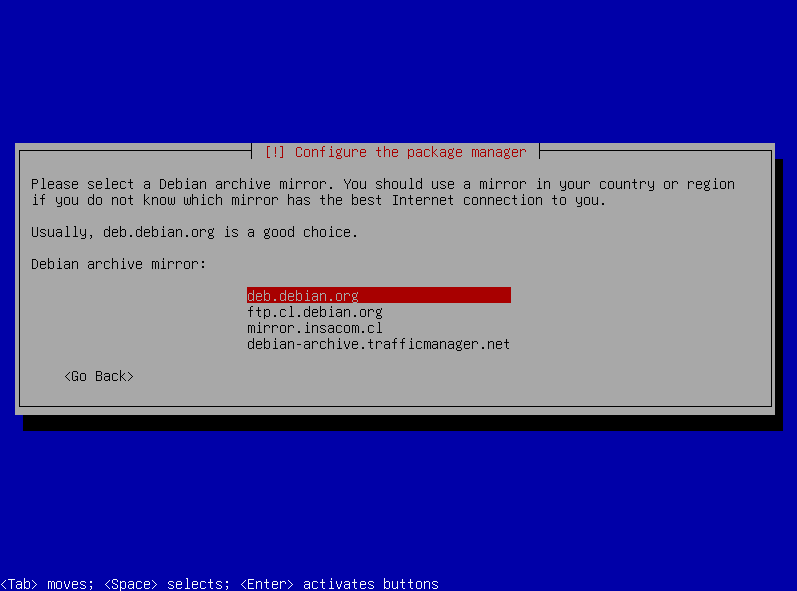


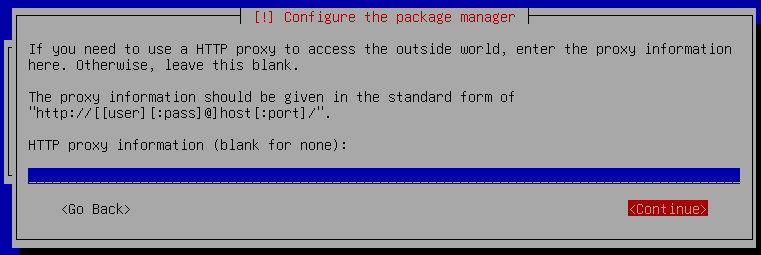
1. Confirmamos los cambios y escribiremos los datos en el dispositivo de almacenamiento



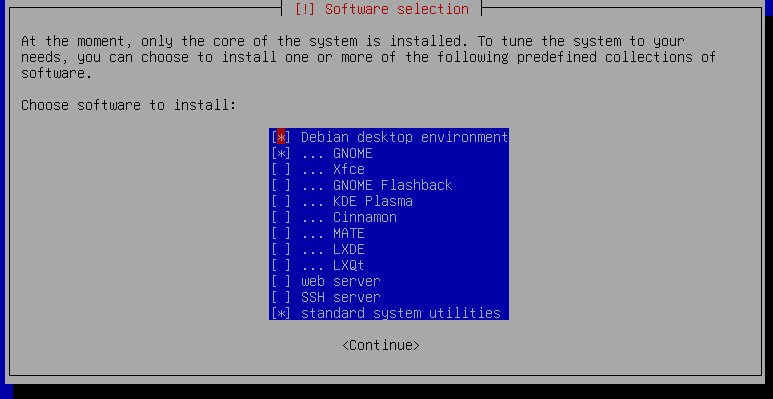
1. Configuramos nuestro gestor de paquetes para que esté conectados a los servidores de nuestro país, luego seleccionamos un mirror y cuando nos pregunte por un proxy dejaremos el campo en blanco



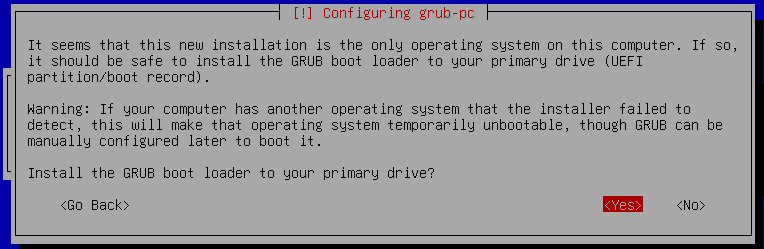




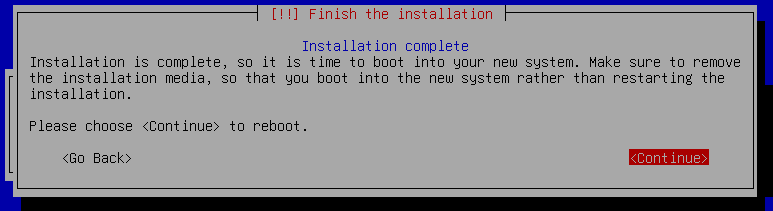
1. Solamente dejamos marcado ssh server y standard system utilities



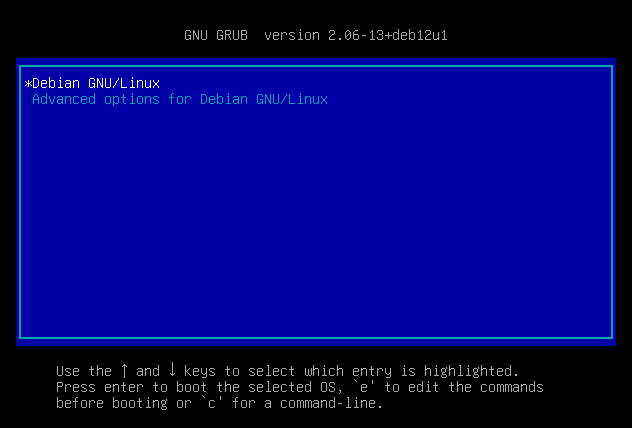
1. Instalaremos en nuestra partición primaria



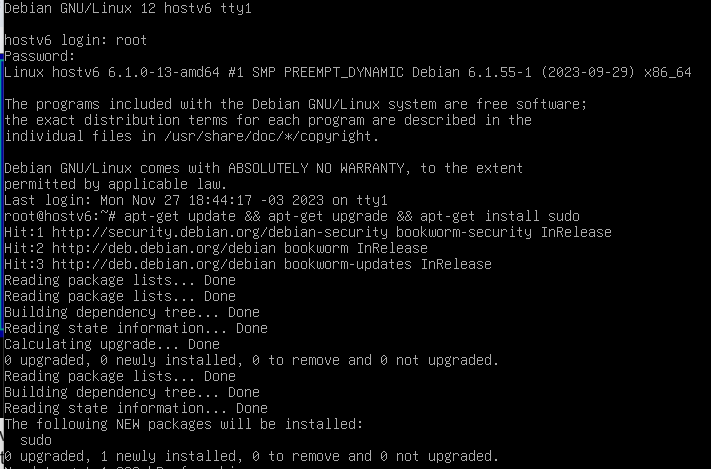
1. Sacaremos nuestro pendrive de nuestro servidor y reiniciamos



1. Entraremos a nuestro grub y seleccionamos nuestro sistema operativo recién instalado



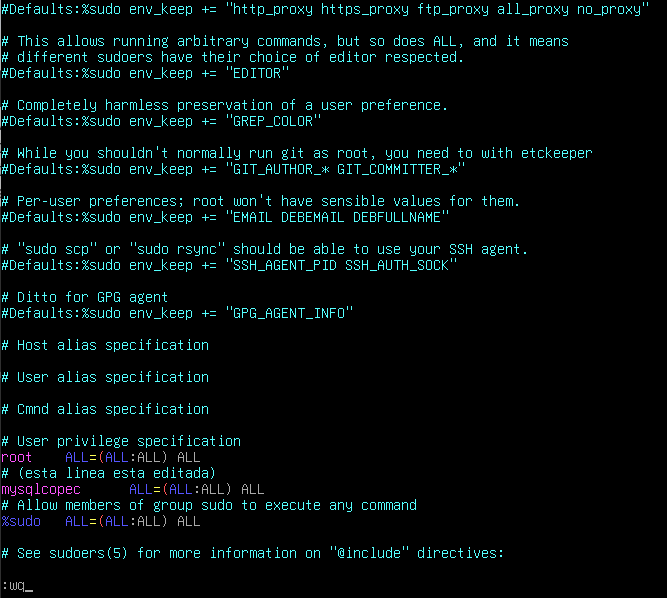
1. Una vez dentro, necesitaremos configurar nuestro archivo sudoers desde nuestra cuenta root, por lo que ingresamos con nuestras credenciales root para actualizar nuestro sistema y luego instalar sudo con el comando ‘apt-get update && apt-get upgrade && apt-get install sudo vim wget curl’



1. Ahora deberemos configurar el archivo sudoers que se encuentra /etc/sudoers usando el comando ‘vim /etc/sudoers’

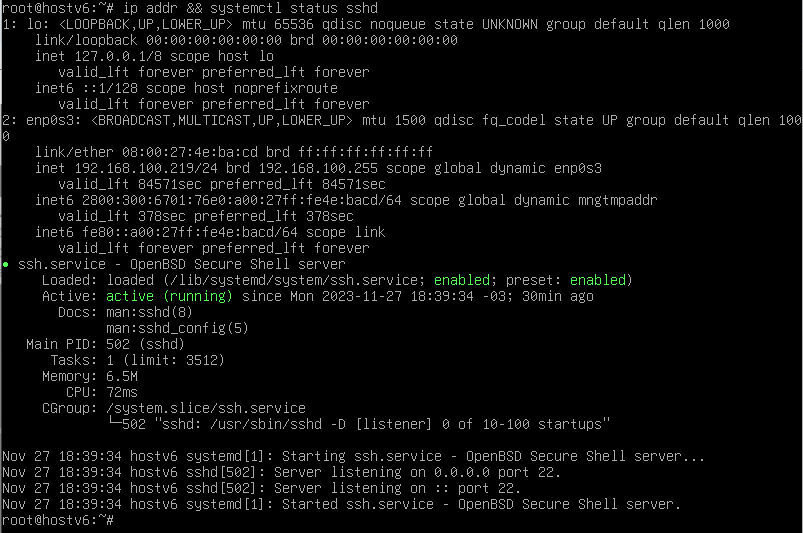


1. Se nos abrirá un editor de texto, deberemos editar el archivo de la siguiente manera:



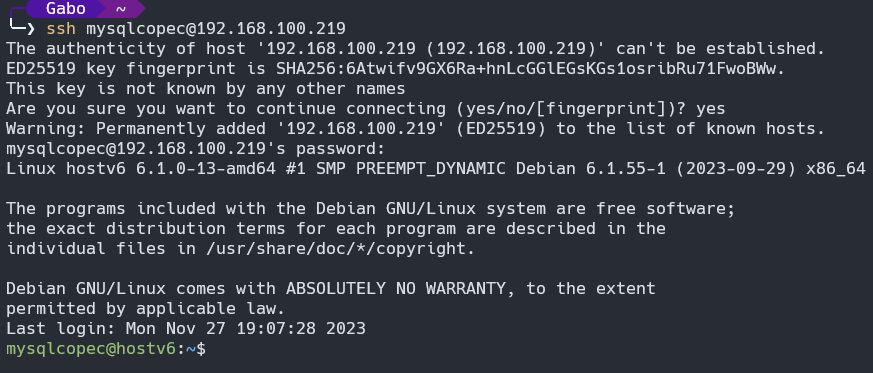
Una vez hayamos añadido nuestro usuario a la lista de sudoers, deberemos apretar ‘:wq!’ para guardar y salir.

1. Usaremos el comando ‘ip addr && systemctl status sshd’ para revisar cual es nuestra ip local y revisar si nuestro servidor ssh está activo

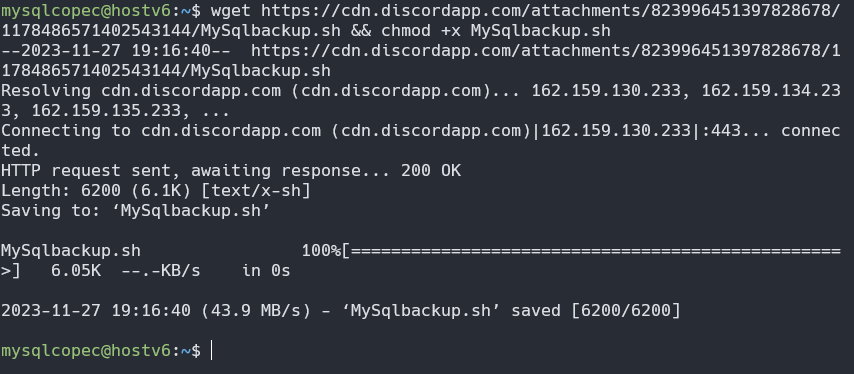


Si todo está en orden, podremos salir de nuestra sesión y conectarnos de forma remota. Si no está nuestro servidor ssh arriba, podemos ejecutar el comando ‘systemctl enable sshd && systemctl start sshd’

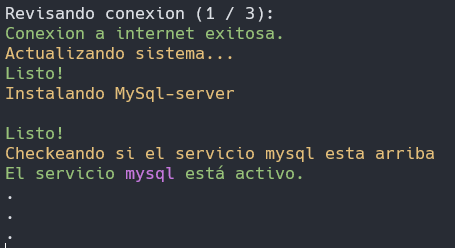
1. Desde nuestro computador local, usaremos el comando mysqlcopec@{ip local dada por ip addr}, escribimos ‘yes’ y nuestra clave para poder iniciar sesión en nuestro servidor de forma remota



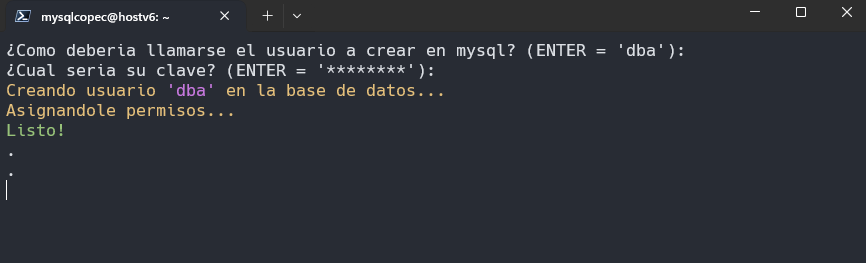
1. ejecutaremos el comando ‘wget <https://cdn.discordapp.com/attachments/823996451397828678/1178486571402543144/MySqlbackup.sh> && chmod +x MySqlbackup.sh’ para descargar nuestro script para recuperar nuestro backup y respaldar



1. Ahora ejecutaremos el comando ‘sudo ./MySqlbackup.sh’ seguido de nuestra clave para ejecutar nuestro script
2. Sabremos que el script comenzará a trabajar cuando aparezcan estos mensajes

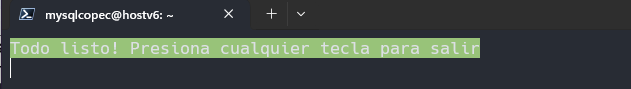


1. El script nos preguntará por las credenciales de nuestro nuevo dba, podemos presionar enter para usar los valores por defecto (no recomendado).

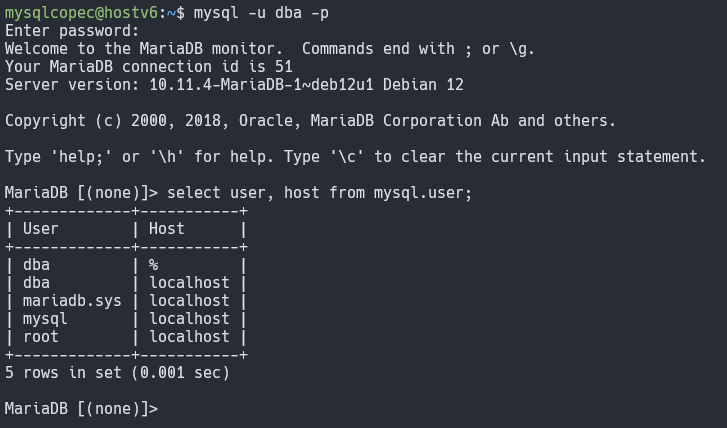


(La clave por default es 2023duoc)

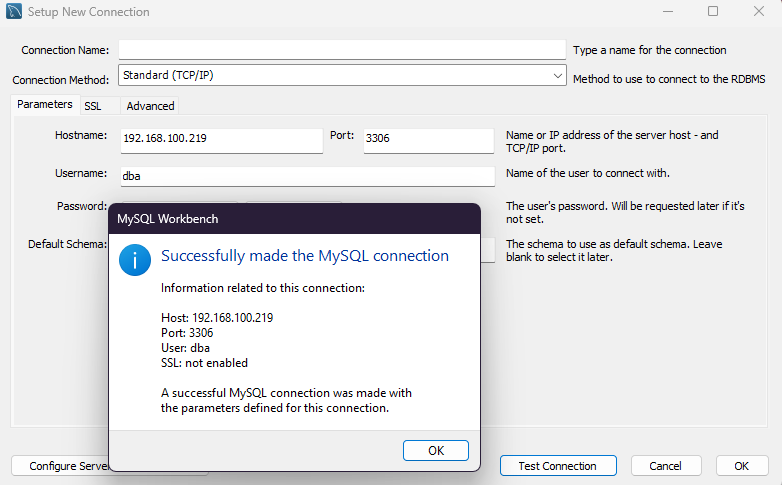
1. Cuando haya finalizado el script, nos avisará con este mensaje



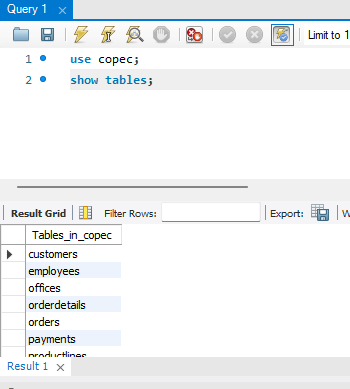
1. Podemos comprobar que nuestro usuario está creado de manera local y remota. Para comprobarlo de manera local, podemos usar el comando ‘mysql -u dba -p’ y digitar nuestra clave



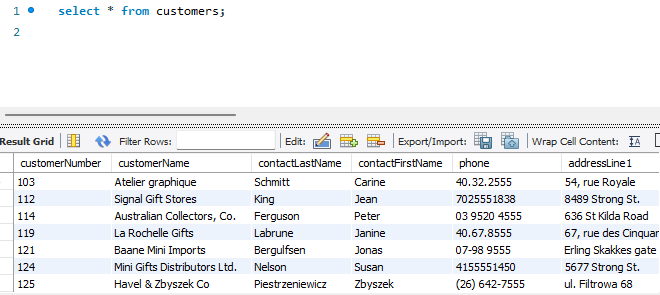
1. También podemos hacer este mismo procedimiento desde un cliente remoto con mysqlworkbench



1. Aprovecharemos de chequear la integridad de los datos desde nuestro cliente



1. Como podemos ver la base de datos está restaurada con sus respectivas tablas, sin embargo no sabemos si la integridad de los datos se ha conservado. Podemos ejecutar alguna consulta para probar:



Pudimos restaurar la base de datos con exitosamente

# Anexos

## Nómina de personal crítico con datos de contacto y reemplazantes

## Alfredo Galdames

## Líder en ciberseguridad informática en DuocUC

## Correo: [Alfredo.galdames@duocuc.cl](mailto:Alfredo.galdames@duocuc.cl)

## Reemplazante: Ignacio Sepúlveda

## Sublíder ciberseguridad

## [nachete@duocuc.cl](mailto:nachete@duocuc.cl)

## Fernando Muñoz

## Analista Forense en radware

## Correo: [munozfe@adware.cl](mailto:munozfe@adware.cl)

## Reemplazante: Daniel Ortega

## Ingeniero junior en ciberseguridad

## Ortegada@adware.cl

## Jean Venegas

## Decano en ciberseguridad de Universidad católica de chile

## Correo: [Je.venegas@catolica.cl](mailto:Je.venegas@catolica.cl)

## Reemplazante: Paula Velásquez

## Docente en universidad católica

## Pau.velazques@catolica.cl

## Nómina de proveedores críticos con datos de contacto

## DuocUC – [www.duocuc.cl](http://www.duocuc.cl) - Av. Esq. Blanca 501 · (2) 2560 6900

## Radware Chile – [www.radware.com](http://www.radware.com) - +56 2 2595 2848

## Universidad catolica de chile - <https://educacionprofesional.ing.uc.cl/> - (+56) 9 5504 4516 / (+56) 9 3353 0870 - Avda. Vicuña Mackenna 4860, Macul - Santiago - Chile