# Plan de recuperación ante desastres COPEC

[28/11/2023]

Seguridad en sistemas computacionales sección 029D

Matías Godoy

Martin Godoy

Jonathan Muñoz

# 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 | 27/11/23 |

## Versión

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versión | Fecha emisión | Cambios realizados | Paginas afectadas | Observaciones |
| 1.0 | 27/11/23 | Documento completo | Documento completo |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Lista de distribución

|  |  |  |
| --- | --- | --- |
| Nombre | Organización | Cargo |
| Matías Godoy | Duoc UC |  |
| Martin Godoy | Duoc UC |  |
| Jonathan Godoy | Duoc UC |  |
|  |  |  |

Tabla de contenido

[Plan de recuperación ante desastres COPEC 1](#_Toc152019051)

[Control de documento 2](#_Toc152019052)

[Preparación 2](#_Toc152019053)

[Versión 2](#_Toc152019054)

[Lista de distribución 2](#_Toc152019055)

[1. Introducción 4](#_Toc152019056)

[1.2. Propósito 4](#_Toc152019057)

[1.3. Alcance 4](#_Toc152019058)

[1.4. Definiciones, acrónimos y abreviaturas 4](#_Toc152019059)

[1.5. Referencias 4](#_Toc152019060)

[1.6. Descripción general del documento 4](#_Toc152019061)

[2. Participantes 4](#_Toc152019062)

[3. Identificación, análisis, y priorización de procesos y servicios críticos TI que forman parte del alcance 4](#_Toc152019063)

[3.1. Procesos de negocio críticos y los servicios/aplicaciones TI que lo soportan 4](#_Toc152019064)

[3.2. Identificación de dependencias de los servicios TI 4](#_Toc152019065)

[3.2. Documentación de arquitectura de sistemas y dependencias 4](#_Toc152019066)

[3.3. Tiempos y puntos de recuperación requeridos y factibles para sistemas y dependencias 4](#_Toc152019067)

[4. Estrategias de recuperación 4](#_Toc152019068)

[5. Procedimiento de alerta, escalamiento, activación y gobierno de la recuperación TI 4](#_Toc152019069)

[5.1. Diagramas de flujo 4](#_Toc152019070)

[5.2. Descripción de equipos y roles 4](#_Toc152019071)

[5.3. Descripción resumida del flujo de escalamiento 4](#_Toc152019072)

[6. Procedimientos de contingencia y recuperación para servidor de base de datos 5](#_Toc152019073)

[6.1. Objetivo 5](#_Toc152019074)

[6.2. Alcance 5](#_Toc152019075)

[6.3. Procedimientos relacionados 5](#_Toc152019076)

[6.4. Desarrollo del procedimiento 5](#_Toc152019077)

[6.5. Detalle de tareas 5](#_Toc152019078)

[7. Anexos 5](#_Toc152019079)

[7.1. Nómina de personal crítico con datos de contacto y reemplazantes 5](#_Toc152019080)

[7.2. Nómina de proveedores críticos con datos de contacto 5](#_Toc152019081)

# Introducción

Este documento, estructurado con un enfoque proactivo, establece los preparativos y procedimientos necesarios para enfrentar emergencias que puedan comprometer la base de datos de la empresa.

El documento se organiza en secciones clave, abordando la identificación de riesgos, la formación de un equipo de respuesta, medidas de respaldo y recuperación de datos, políticas de seguridad, simulacros y ejercicios de entrenamiento, y acuerdos con proveedores de servicios de recuperación. Estas secciones están diseñadas para ofrecer una guía integral que permita a Copec anticiparse y responder eficazmente ante desafíos informáticos críticos.

## 1.2. Propósito

El propósito fundamental de este plan es garantizar la continuidad operativa de Copec en situaciones de emergencia que puedan afectar la integridad de su base de datos. Este documento se redacta con el objetivo de mitigar y evitar los impactos negativos y proporcionar una respuesta eficiente, rápida y coordinada ante eventos imprevistos que podrían comprometer la disponibilidad y confidencialidad de la información crítica de la empresa.

## 1.3. Alcance

Este plan abarca las operaciones relacionadas con la gestión de inventario, pagos, administración de cuentas de usuarios y el funcionamiento en general de las empresas Copec. Incluye, pero no se limita a, incidentes como pérdida de datos (de hecho, uno de los objetivos principales es mitigar la mayor pérdida de datos posibles), intrusiones, fallos de hardware, desastres naturales y otros eventos imprevistos que puedan comprometer la disponibilidad y confidencialidad de la información.

Este plan se aplicará a todos los niveles de la organización, desde el personal encargado de la administración de la base de datos hasta los responsables de la toma de decisiones estratégicas. La implementación y revisión periódica de este plan se consideran aspectos fundamentales para garantizar su efectividad continua y su capacidad para adaptarse a la evolución de las amenazas y tecnologías.

En resumen, este documento busca establecer un marco sólido y proactivo para la gestión de crisis.

## 1.4. Definiciones, acrónimos y abreviaturas

* **Desastre Informático**: Un evento que interrumpe significativamente las operaciones normales de los sistemas informáticos, resultando en pérdida de datos o funcionalidad.
* **Backup**: Copia de seguridad de datos críticos almacenada fuera del sitio principal para su recuperación en caso de pérdida.
* **Failover**: Proceso automático o manual para cambiar a un sistema de respaldo cuando el sistema principal falla.
* **Sistema de Continuidad de Negocio**: Conjunto de procedimientos y recursos para mantener las operaciones comerciales durante y después de un desastre.
* **LAN:** Red de área local
* **Raid:** Conjunto de dispositivos de almacenamientos redundante
* **UPS:** Fuente de alimentación de corriente ininterrumpida
* **BD,DB,BBDD:** Base de datos
* **SQL:** Lenguaje de consultas estructurado
* **MIRROR:** Servidor alternativo que busca ofrecer el mismo contenido que ofrece un servidor oficial
* **SSH:** Protocolo de red que sirve para conectarse de manera remota a una maquina
* **UEFI:** Interfaz unificada de firmware extensible
* **Firmware:** Conjunto de instrucciones que establece la lógica de más bajo nivel de una máquina, controla los circuitos del dispositivo
* **RAM:** Memoria de acceso aleatorio
* **CPU:** Unidad central de procesamiento
* **SSD:** Unidad de estado sólido (Almacenamiento)
* **HDD:** Disco duro
* **MB:** Placa madre
* **SCRIPT:** Pequeño conjunto de instrucciones para automatizar o facilitar procesos
* **IP:** Protocolo de internet que provee una dirección única en la red
* **IDS:** Sistema de detección de intrusos
* **IPS:** Sistema de prevención de intrusos
* **OS:** Sistema operativo

## 1.5. Referencias

* Ubuntu: [Enterprise Open Source and Linux | Ubuntu](https://ubuntu.com/)
* Ubuntu server: [Get Ubuntu Server | Download | Ubuntu](https://ubuntu.com/download/server)
* Información de empresas copec:
  + [Descripción general - Copec RI (empresascopec.cl)](https://investor.empresascopec.cl/gobierno-corporativo/descripcion-general/)
  + [Empresas Copec S.A. | Gobierno corporativo](https://www.empresascopec.cl/gobierno-corporativo/)
* Hardware de servidor
  + CPU: [Procesador Intel® Xeon® Platinum 8452Y](https://www.intel.la/content/www/xl/es/products/sku/231761/intel-xeon-platinum-8452y-processor-67-5m-cache-2-00-ghz/specifications.html)
  + MB: [MS73-HB2 (rev. 1.x) | Server Motherboard - GIGABYTE Global](https://www.gigabyte.com/Enterprise/Server-Motherboard/MS73-HB2-rev-1x)
  + RAM: [KSM48R40BD4TMM-64HMR-B.ai (kingston.com)](https://www.kingston.com/datasheets/KSM48R40BD4TMM-64HMR.pdf)
  + SSD: [DC1500M Enterprise U.2 NVMe Solid-State Drive 960GB-7.6TB - Kingston Technology](https://www.kingston.com/en/ssd/dc1500m-data-center-ssd)
* Otros
  + [Descripción de puestos directivos: cuáles hay | Indeed.com México](https://mx.indeed.com/orientacion-profesional/como-encontrar-empleo/descripcion-puestos-ejecutivos#:~:text=Quienes%20desempe%C3%B1an%20un%20puesto%20directivo,resultados%20deseados%20en%20la%20organizaci%C3%B3n.)

## 1.6. Descripción general del documento

Este es un documento integral diseñado para proporcionar instrucciones y guiar detalladamente tanto al equipo de copec como a la organización acerca de cómo actuar frente a ciertas situaciones de desastres que puedan afectar la integridad, disponibilidad y confidencialidad de los servicios de la base de datos de Copec

# Participantes

* Matías Godoy – Ingeniero senior Desarrollos Copec
* Martin Godoy - Ingeniero líder de desarrollo informático
* Jonathan Muñoz – Jefe de administración de base de datos
* Hernán Villagrán Tapia – Oficial de seguridad de la información
* Pamela Harris Honorato – Subgerenta de asuntos corporativos
* Rodrigo Huidobro Alvarado – Gerente de administración y finanzas
* Eduardo Navarro Beltrán – Gerente General
* Roberto Angelini Rossi – Presidente directorio

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

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

Los procesos que pueden verse afectados ante un posible desastre pueden verse afectados si el servidor de base de datos es el afectado, los negocios críticos relacionados con los servicios podrían incluir:

* Proceso de registro de transacciones financieras
  + La base de datos contiene registros financieros utilizados por las aplicaciones de copec
* Proceso de gestión de inventarios
  + La base de datos contiene los registros de inventario por la aplicación de inventario y pañol de copec
* Procesos de gestión de pedidos y facturación
  + El sistema depende de la base de datos para poder gestionar los pedidos, facturaciones y procesos asociados

## 3.2. Identificación de dependencias de los servicios TI

Las dependencias criticas incluyen:

* Arquitectura del software:
  + Aplicaciones web de clientes
    - Las páginas dependen de la base de datos para poder obtener, actualizar y manipular la información del cliente
  + Sistemas de reportes y de analítica
    - Los sistemas de reportes y de análisis dependen de la base de datos para poder obtener la información esencial para este proceso pueda operar
  + Sistema de gestión de usuarios y accesos
    - Este sistema necesita acceder a la base de datos para poder accionar las consultas necesarias y discriminar los accesos de usuario y gestionar un CRUD dentro de los sistemas
* Hardware:
  + Todos los servidores y firewalls que contienen los sistemas anteriormente mencionados y la base de datos.
  + Los servidores deben contener el siguiente hardware:
    - CPU: [Intel® Xeon® Platinum 8452Y](https://www.intel.la/content/www/xl/es/products/sku/231761/intel-xeon-platinum-8452y-processor-67-5m-cache-2-00-ghz/specifications.html)
    - MB: [MS73-HB2 (rev. 1.x) | Server Motherboard - GIGABYTE Global](https://www.gigabyte.com/Enterprise/Server-Motherboard/MS73-HB2-rev-1x)
    - RAM: x16 módulos [KSM48R40BD4TMM-64HMR-B.ai (kingston.com)](https://www.kingston.com/datasheets/KSM48R40BD4TMM-64HMR.pdf)
    - SSD-BD: [DC1500M Enterprise U.2 NVMe Solid-State Drive 960GB-7.6TB - Kingston Technology](https://www.kingston.com/en/ssd/dc1500m-data-center-ssd)
    - SSD: [Data Center DC1000B – M.2 (2280) NVMe Server Boot Drive (SSD) – 240GB and 480GB - Kingston Technology](https://www.kingston.com/en/ssd/dc1000b-data-center-boot-ssd)
    - FUENTE: [HPE Performance Power Supplies Data sheet](https://www.hpe.com/psnow/doc/PSN5188937WWEN.pdf?jumpid=in_pdp-psnow-dds)

\*El servidor usara el sistema operativo de Ubuntu server

## 3.2. Documentación de arquitectura de sistemas y dependencias

La arquitectura de sistemas y dependencias debe estar exhaustivamente documentada, mostrando en detalle las configuraciones del servidor de base de dato, las conexiones que usara y sus dependencias

Diagrama

Descripción generada automáticamente

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

* RTO (Tiempo objetivo de recuperación)
  + El tiempo objetivo de recuperación puede ser bastante variable según el volumen de datos que se tenga que recuperar de la base de datos. Se estima que, si el volumen de datos es muy denso, el tiempo de recuperación seria de alrededor de 8 horas en un servidor normal. Sin embargo, considerando el hardware a utilizar en el servidor, se puede afirmar que el tiempo de recuperación en todos los servicios seria de un máximo de 3 horas.
* RPO (Punto de recuperación)
  + Podemos considerar recuperado el sistema una vez se haya restaurado la base de datos completamente y que todas las pruebas hechas a los sistemas hayan sido aprobadas.

# Estrategias de recuperación

Se deberán respaldos periódicamente a la base de datos mediante el uso de programas como cronjob en el servidor, en el cual se ejecutará una serie de instrucciones que hará lo siguiente 2 veces por día:

* Hará un respaldo de la base de datos completo, manteniendo la seguridad e integridad de los registros.
* Ese respaldo será subido a un servidor de Google drive, asegurando que este archivo estará en un lugar seguro y en un ambiente controlado, esta carpeta de Google drive solamente podrá ser accedida por las credenciales del Administrador de base de datos

Adicionalmente, se mantendrán en el inventario unidades de almacenamiento adicionales que contengan el sistema operativo instalados, siendo clasificados por el tipo de servidor en el que se usarán; Por ejemplo: Un con Ubuntu Server y MySql+OpenSSH instalados y configurados, otra con Apache o nginx+NodeJS+Python+OpenSSH instalados para los servidores web, servidores backend o servidores de balanceo de carga. Esto con la finalidad de poder agilizar la reintegración del servidor sin tener que pasar por los tiempos de carga al momento de tener que instalar un nuevo sistema operativo

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

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamenteConsiderando la geografía y el estado del país en el que opera Copec, debemos considerar distintos tipos de alerta, ya que como bien se sabe Chile es un país Sísmico, con mucha diversidad climática y polarizado en cuanto a la política, por lo que se harán distintos procedimientos de alertas según el contexto. Ayudando a este punto, también se contarán con sistemas de prevención y detección de intrusos tanto por red y en puntos físico, si estos sistemas llegasen a activarse, el gobierno corporativo dentro de lo que sería Empresas Copec sufrirán de una mutación en cuanto a las escalas y alcances que tendrá cada equipo y departamento, en el cual comité de seguridad de la información estaría por sobre el equipo ejecutivo hasta que se cumpla el RPO.

## 5.1. Diagramas de flujo

Diagrama

Descripción generada automáticamente

## 5.2. Descripción de equipos y roles

* **Comité de directores:** El Comité de Directores está a cargo de proponer al Directorio los nombres de los auditores externos y clasificadores privados de riesgo, para que sean sugeridos y aprobados en la respectiva Junta Ordinaria de Accionistas, y revisar periódicamente los informes presentados por los auditores externos, los estados financieros de la Compañía, los informes de gestión de riesgo, las transacciones con empresas relacionadas, las políticas de remuneraciones y los planes de compensación de gerentes, principales ejecutivos y trabajadores, entre otras materias. Está constituido por tres integrantes, de acuerdo con lo indicado en el artículo 50 bis de la Ley N° 18.046, los que son elegidos entre los miembros del Directorio, asegurando que el director Independiente, quien es designado con los votos de los accionistas minoritarios.
  + Presidenta del comité de directores
  + Director(es)
* **Directorio**: El Directorio es responsable de definir y evaluar la estrategia general de la Compañía en el corto, mediano y largo plazo; revisar, aprobar y monitorear las decisiones financieras fundamentales, como la política de dividendos y la estructura de capital; controlar la gestión de las operaciones de la empresa; analizar grandes proyectos de inversión, transacciones y ventas de activos; asegurar los recursos necesarios para la debida gestión de riesgos; revisar y aprobar los estados financieros preparados por la Administración; velar por el cumplimiento de la ley y de las normas de autorregulación; monitorear la relación con autoridades y agentes clave del mercado; mantener permanentemente informados a los accionistas; seleccionar al gerente general y evaluar su desempeño, teniendo facultades para removerlo y supervisar su reemplazo, y asesorar en la selección, evaluación, desarrollo y compensación de los principales ejecutivos de la Compañía, entre otras funciones.
  + Presidente de directorio
  + Vicepresidente de directorio
  + Director(res)
* **Equipo ejecutivo:** Los directivos son responsables de tomar decisiones que afectan a la dirección y el rumbo de la organización. Parte de estas tareas incluyen evaluar opciones, analizar datos, considerar factores internos y externos, y elegir la mejor acción para lograr los objetivos de la empresa. son responsables de definir y comunicar la estrategia global de la organización, por lo que deben de examinar las oportunidades de crecimiento, analizar el entorno competitivo, establecer objetivos estratégicos y diseñar planes de acción para lograrlos.
* **Comité de seguridad de la información**: El Comité de Seguridad de la Información está conformado por tres integrantes, los que son elegidos por el Gerente General con el objetivo de implementar las políticas, normas y procedimientos establecidos en el Modelo de Seguridad de la Información, y velar por su cumplimiento.
  + Oficial de seguridad de la información
  + Subgerente de asuntos corporativos
  + Gerente de administración y de finanzas
  + Analista de estudios Senior
  + Analista contable Senior
* **Equipo de desarrollo:** trabajan en servicios de diseño de sistemas informáticos, para editores de software y en diversas industrias de fabricación de dispositivos informáticos. Estos ingenieros trabajan para identificar problemas con programas y aplicaciones e informarlos o corregirlos.
  + Jefe de administración de base de datos
  + Jefe ingeniería de desarrollo informático
  + Jefe de diseños y de usabilidad de usuario
  + Jefe de networking y comunicaciones de red

## 5.3. Descripción resumida del flujo de escalamiento

El flujo de escalamiento comenzara cuando a ejercerse cuando se entre en estado de alerta, el flujo hará cambiar los puestos entre el comité de seguridad de la información y el equipo directivo, haciendo que este último tenga menor influencia y menos poder en la toma de decisiones de la empresa hasta que el estado de alerta de desastre se acabe y Copec vuelva a operar con normalidad

# Procedimientos de contingencia y recuperación para servidor de base de datos

### 6.1. Objetivo

El objetivo de este procedimiento es recuperar la integridad de los datos de la base de datos y volver al funcionamiento habitual en el menor tiempo posible, mediante la manera más segura. Haciendo uso de las herramientas a alcance de los trabajadores y los protocolos que se han preparado para estas situaciones.

### 6.2. Alcance

Tal como se menciono en los diagramas definidos en el punto 5, cuando se entre en un estado de alerta, el procedimiento variara un poco según el tipo de alerta. En el que puede variar si la alerta es producida por un desastre natural, algún tipo de manifestación social alrededor del recinto en el cual se encuentra el servidor, o algún tipo de ataque; Apenas se entre en estado de alerta, el poder del equipo de comité de seguridad de la información ascenderá y podrá tomar decisiones pasando por alto la burocracia que pueda existir, dándole mas libertad para poder ejecutar las acciones necesarias que requiera para poder mitigar esta situación lo antes posible.

### 6.3. Procedimientos relacionados

En la mayoría de los procedimientos descritos por el diagrama de flujos, implica hacer una revisión de hardware al servidor, en el que es muy probable que se tenga que restaurar el dispositivo de almacenamiento y la placa madre, de ser así el caso, el procedimiento se debe seguir al pie de la letra para poder perder el menor tiempo posible

### 

### 6.4. Desarrollo del procedimiento

Diagrama

Descripción generada automáticamente

#### 6.4.1. Fase de transición a operación en contingencia (failover).

El estado de failover en este documento se presentará cuando se entre en un estado de desastre, ascendiendo en la escala de gobierno al equipo del comité de seguridad de la información, dándole mas libertades para poder ejecutar los procedimientos de una manera más rápida y eficaz

#### 6.4.2. Fase a operación en contingencia

El estado de operación en contingencia en este documento presenta el que se debe hacer en el estado de alerta, como se ha indicado con anterioridad en los otros puntos, el procedimiento puede variar ligeramente según el tipo de desastre, Sin embargo todos los procedimientos buscan mantener la integridad de los datos y del servidor, buscando la manera más optima, rápida y eficiente de poder volver a la normalidad asegurándose de que todo está en orden.

Es posible de que las situaciones sean estas:

* Desastre natural
  + Este punto es cuando puede ocurrir un terremoto de gran escala, lluvias de gran intensidad, etc. El procedimiento aquí es verificar la integridad del hardware, si algún componente ya no esta apto para poder seguir trabajando se debe reemplazar por una de las mismas características. En caso de que la unidad de almacenamiento este fallando, se debe reemplazar por otra del mismo modelo y que contenga el software preinstalado, estas unidades están guardades en lo que sería el inventario del recinto.
* Manifestaciones.
  + Si alguna manifestación que se encuentre alrededor del recinto logra afectar el funcionamiento de los servicios de copec, el procedimiento dice que se debe llamar a las debidas autoridades para tomar acciones, luego se debe hacer pruebas de networking y de servicios para asegurarse de que todo esté en orden
* Ataque informático o activación de detección de intrusos
  + Si algún IDS llegase a detectar algo sospechoso, o ya es obvio que existe algún tipo de ataque hacia copec, el comité de seguridad debe llegar al poder lo más rápido posible para tomar las debidas acciones, estas acciones deben ser aplicadas desde lo que sería el Harding:
    - Establecer política de contraseñas
    - Cerrar puertos que no estén en uso
    - Cerrar servicios que no estén en uso
    - Restringir las conexiones
    - Cambiar los puertos que se usan por defecto
    - No dar permisos de administrador a cualquier cuenta
    - Mantener cada servicio en un servidor de forma independiente
    - Activar ips dinámicas y cambiar el subhost que existe en las redes de los servidores
  + También, los dispositivos de almacenamiento y placas madre de los servidores que estén siendo victimas de un ataque deberán ser cambiados para asegurar de que en caso de que haya un rootkit instalado o algún otro tipo de programa maligno sea eliminado por completo. Luego se deberá ejecutar el mismo procedimiento de reinstalación de sistemas que siguen el resto de los procedimientos

Por cada vez que se saca alguna unidad de almacenamiento para poder reponer el ambiente de producción de algún ambiente, se deben producir más unidades con los sistemas preinstalados para el respectivo ambiente que fue repuesto, esto con el fin de asegurar stock ante un posible futuro evento de desastre.

Una vez se haya solucionado el desastre ocurrido, se deberán hacer de manera obligatoria una serie de pruebas en los ambientes y servidores para asegurarse de que todos los servicios van a funcionar de manera correcta a la entrada a producción.

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

Una vez las pruebas hayan sido aprobadas por completo, los equipos ejecutivos y el comité de seguridad podrán volver a sus puestos habituales y pueden volver a funcionar con completa normalidad.

### Detalle de tareas

Una vez el comité de seguridad obtiene poder, se debe dar la orden de manera de inmediata de verificar la integridad de los servidores.

Si se llegase a necesitar un cambio de almacenamiento, este es el procedimiento que se debe seguir:

1. Cambiamos nuestro disco duro (sea porque este infectado, hay un ataque informático o simplemente quedo en mal estado después de un desastre natural).
2. Se da la orden al pañolero que de manera paralela haga una instalación nueva de Ubuntu server con los programas necesarios para usar una base de datos para una próxima alerta de desastre.
3. Iniciamos sesión en nuestro servidor Ubuntu con las credenciales que se usaran por defecto (user: marting | pass: seguridad)

Texto

Descripción generada automáticamente

1. Checkeamos que el servicio de SSH este en ejecución y revisamos cual es nuestra IP interna

Texto

Descripción generada automáticamente

1. Sabiendo esta información, podemos operar de forma remota desde nuestro equipo de comodidad.

Pantalla de computadora con letras

Descripción generada automáticamente con confianza media

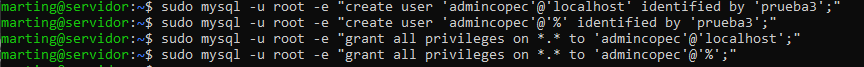
1. Ahora podemos instalar nuestro servidor MySQL usando el comando ’sudo apt install mysql-server’Texto

   Descripción generada automáticamente
2. Se debe configurar el archivo que se encuentra en el directorio ‘/etc/mysql/mysql.conf.d/mysqld.conf’ con el editor de preferencia como se indicara en la foto con los permisos root

Texto

Descripción generada automáticamente

1. Ahora deberemos agregar el usuario en la base de datos para poder operar en ella, por lo que ejecutaremos una serie de instrucciones que estarán en la siguiente imagen. Usaremos las credenciales user: ‘admincopec’ | pass: ‘prueba3’ para poder acceder a nuestra base de datos



1. Ahora debemos reiniciar nuestra base de datos para aplicar nuestros cambios usando el comando ‘sudo systemctl restart mysql’. Adicionalmente podemos consultar el estado de nuestra base de datos usando el comando ‘sudo systemctl status mysql’.

Texto

Descripción generada automáticamente

1. Podemos probar el funcionamiento de nuestras credenciales tanto de manera local como remota, tal como se indicarán en las siguiente fotos Texto

   Descripción generada automáticamente
2. Ahora aplicaremos el respaldo de nuestra base de datos de forma remota, por lo que debemos usar los programas GIT y MySqlWorkbench para poder obtener nuestros respaldos de base de datos y poder conectarnos y respaldar los datos, desde nuestra cmd clonaremos el siguiente repositorio: https://github.com/hhorak/mysql-sample-db.git

Texto

Descripción generada automáticamente

1. Una vez clonado el repositorio, nos conectamos a nuestra base de datos usando el cliente MySQLWorkbench

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Podemos ver que estamos conectados a la base de datos usando la misma IP que usamos para conectarnos de forma remota mediante SSH ya que el resultado de la consulta ‘show tables;’ nos arroja la misma información como si lo estuviésemos haciendo desde la maquina local

1. Ahora debemos importar nuestro respaldo que clonamos desde nuestro repositorio

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

La carga es de 167MB por lo que es normal que se tarde mas de lo usual.

1. Ahora nos iremos a la segunda pestaña para poder comenzar la importación de datos

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Al final deberá salir un mensaje como ‘05:14:02 Import of D:\Duoc\tercerAnnio\SegundoSemestre\ciberseguridad\prueba4\mysql-sample-db\mysqlsampledatabase.sql has finished’
2. Ya con esto, podemos verificar si la base de datos que hemos respaldado desde MySqlWorkbench

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Para finalizar, deberemos configurar cronjob para poder hacer tareas periódicas de generar un respaldo de nuestra base de datos cada 12 horas y subir ese respaldo a github

Texto

Descripción generada automáticamente

# Anexos

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

* Elliot Alderson – Experto en ciberseguridad – [mr.robot@ecorp.com](mailto:mr.robot@ecorp.com)
* Thomas A. Anderson – WhiteHat Hacker y expert en ciberseguridad – [neo@matrix.com](mailto:neo@matrix.com)
* Lain Iwakura – Ingeniera en Redes y Magister en ciencias computacionales – lain.iw@serialexperiments.jp
* Itaru Hashida – Analista Forense en Future Gadget Laboratory – daru@steinsgate.jp

### 7.2. Nómina de proveedores críticos con datos de contacto

* Allsafe Cybersecurity
  + Tipo de Servicio/Producto: Compañía privada de ciberseguridad
  + Contacto Principal: Gideon Goddard – gideongoddard@allsafe.us - +56912345678
* Deous Group
  + Tipo de Servicio/Producto: Compañía de gubernamental de ciberseguridad
  + Contacto Principal: Zhi Zhang – Zhang@deous.cn - +56987654321
* Yorha
  + Tipo de Servicio/Producto: Compañía de ciberseguridad
  + Contacto Principal: Nier Emil – nier@yorha.jp - +56943215678