



TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Implementación de Servidor CentOS con norma ISO-
IEC 27001:2013 para seguridad de Intranet de CFE
Zona Cuautitlán

Informe Técnico de Residencias Profesionales

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Para obtener el título de

Ingeniería en Sistemas Computacionales

Especialidad
Auditoría y Seguridad Informática

Presenta(n):

Miguel Ángel Medina Nolasco

Matricula: 201910014

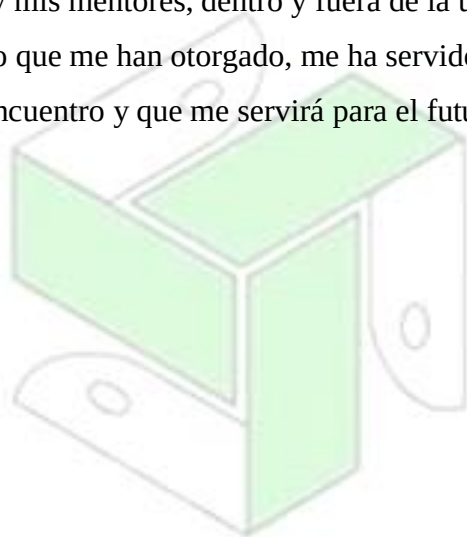
Coacalco de Berriozábal, Julio /2024

AGRADECIMIENTOS

Doy gracias a Dios por permitirme experimentar el camino del esfuerzo y recompensas dentro de mi carrera universitaria, así como los éxitos y caídas que haya tenido, porque de estas experiencias evoluciono y me supero.

Quiero agradecer a mi familia por brindarme apoyo incondicional en todo aspecto de mi vida, por el techo, la comida y cualquier situación que me hiciera resistir más durante mi vida.

Agradezco a mis amigos y mis mentores, dentro y fuera de la universidad, cuya ayuda, colaboración o conocimiento que me han otorgado, me ha servido para estar en el lugar que me encuentro y que me servirá para el futuro.



TESCO

RESUMEN

Las Redes informáticas están presentes en toda tecnología de comunicación, desde en el intercambio y transmisión de datos de los teléfonos móviles y ordenadores, hasta grandes sistemas de dispositivos, cuales operan todos los procesos de información y transferencia de grandes compañías o empresas públicas y privadas.

Durante la siguiente documentación en este reporte, se ha descrito y registrado resultado obtenidos de entrevistas, cuestionarios, FODAS y análisis de riesgos, sintetizados para encontrar vulnerabilidades y asignar recomendaciones y estrategias para subsanar, mitigar, prevenir o evitar incidentes.

Con ayuda de la norma ISO-IEC 27001:2013 se ha logrado implementar un servidor de monitoreo para la seguridad de la red interna o intranet de CFE zona Cuautitlán, recopilado información, planteando y estableciendo un control de seguridad de la información que tiene una escalabilidad, beneficios enfocados a conocer más aspectos que pueden ser monitoreados de los equipos conectados y haciendo uso de una herramienta gratuita.

Finalmente se añaden recomendaciones de mejora y apoyo de métricas basados en la misma norma ISO-IEC 27001:2013 y el marco de trabajo COBIT 4.0.

TESCO

ÍNDICE DE CONTENIDOS

CONTENIDO

AGRADECIMIENTOS	2
RESUMEN	3
ÍNDICE DE CONTENIDOS	4
INTRODUCCIÓN	14
CAPÍTULO I GENERALIDADES DEL PROYECTO.....	16
DESCRIPCIÓN DE LA EMPRESA.....	17
Razón social; Comisión Federal de Electricidad	17
Organigrama	17
Misión	18
Visión.....	19
Filosofía y/o Valores	19
Breve historia de la empresa.....	19
PROBLEMA A RESOLVER.....	20
OBJETIVOS	22
Objetivo general.....	22
Objetivos específicos.....	22
JUSTIFICACIÓN	23
CAPÍTULO II MARCO TEÓRICO	24
Marco Histórico - Contextual.....	25
Marco Conceptual	26
Marco Metodológico.....	34
CAPÍTULO III DESARROLLO	35
3.1 OBJETIVO ESPECÍFICO	36
3.1.1 ACTIVIDAD A REALIZAR	36
DESCRIPCIÓN DE LA ACTIVIDAD	36
RESULTADO DE LA ACTIVIDAD.....	36
3.1.2. ACTIVIDAD A REALIZAR	40
DESCRIPCIÓN DE LA ACTIVIDAD	40
RESULTADO DE LA ACTIVIDAD.....	40
3.1.3. ACTIVIDAD A REALIZAR	43
DESCRIPCIÓN DE LA ACTIVIDAD	43
RESULTADO DE LA ACTIVIDAD.....	43
3.2.OBJETIVO ESPECÍFICO	50

3.2.1. ACTIVIDAD A REALIZAR	50
DESCRIPCIÓN DE LA ACTIVIDAD	50
RESULTADO DE LA ACTIVIDAD.....	50
3.2.2. ACTIVIDAD A REALIZAR	57
DESCRIPCIÓN DE LA ACTIVIDAD	57
RESULTADO DE LA ACTIVIDAD.....	57
3.2.3. ACTIVIDAD A REALIZAR	68
DESCRIPCIÓN DE LA ACTIVIDAD	68
RESULTADOS DE LA ACTIVIDAD	68
CAPÍTULO IV RESULTADOS	86
4.1. OBJETIVO ESPECÍFICO.....	87
4.1.1. ACTIVIDAD A REALIZAR	87
DESCRIPCIÓN DE LA ACTIVIDAD	87
RESULTADO DE LA ACTIVIDAD.....	87
4.1.2. ACTIVIDAD A REALIZAR	101
DESCRIPCIÓN DE LA ACTIVIDAD	101
RESULTADO DE LA ACTIVIDAD.....	101
4.1.3. ACTIVIDAD A REALIZAR	120
DESCRIPCIÓN DE LA ACTIVIDAD	120
RESULTADO DE LA ACTIVIDAD.....	120
4.1.4. ACTIVIDAD A REALIZAR	171
DESCRIPCIÓN DE LA ACTIVIDAD	171
RESULTADO DE LA ACTIVIDAD.....	171
CONCLUSIONES	197
COMPETENCIAS DESARROLLADAS	199
FUENTES DE INFORMACIÓN.....	201
ANEXOS	204

ÍNDICE DE IMÁGENES

Imagen 1 Organigrama general de CFE Zona Cuautitlán, imagen1.	17
Imagen 2 Organigrama general de CFE Zona Cuautitlán, imagen2.	17
Imagen 3 Organigrama general de CFE Zona Cuautitlán, imagen3.	18
Imagen 4 Organigrama general de CFE Zona Cuautitlán, imagen4.	18
Imagen 5 Calendario de actividades en base al objetivo específico durante la Residencia Profesional.	34
Imagen 6 Calendario de actividades en base al objetivo específico durante la Residencia Profesional	34
Imagen 7 Relación Poco personal en TIC's con otras vulnerabilidades.	70
Imagen 8 Propuesta de modelo de madures de los procesos.	75
Imagen 9 Página principal de WireShark.	88
Imagen 10 Descargas para WireShark.	89
Imagen 11 Videos en la documentación de WireShark.	89
Imagen 12 Página web Zabbix definir limites en problemas.	92
Imagen 13 Manual de zabbix sección servidor.....	93
Imagen 14 Selección descarga e instalación de zabbix.	94
Imagen 15 Selección descarga e instalación de zabbix imagen 2.	94
Imagen 16 Manual de zabbix sección Agente.	95
Imagen 17 Ejemplo de Dashboard en Zabbix.....	95
Imagen 18 Breve manual acerca de los sensores en PRTG.	97
Imagen 19 Página principal de PRTG PAESSLER.	97
Imagen 20 Sección Soluciones en redes de PRTG en página web.	98
Imagen 21 Resumen de los temas de supervisión de software de red.....	98
Imagen 22 Puertos que usa zabbix.	102
Imagen 23 Página de descarga de CentOS 9 Stream.	103
Imagen 24 Página de descarga de CentOS 9 Stream imagen 2.....	104
Imagen 25 Configuración de CentOS pre instalación.....	105
Imagen 26 Destino de instalación de CentOS pre instalación	106
Imagen 27 Selección de software de CentOS pre instalación.....	106
Imagen 28 Selección de software de CentOS pre instalación imagen 2.	107
Imagen 29 Host Name para CentOS.	107
Imagen 30 Asignación de usuario normal para CentOS.....	108
Imagen 31 Asignación de usuario root para CentOS.....	108
Imagen 32 Cambios en APR-util versión 1.6.0 o superior.	110
Imagen 33 Página para la descarga de expat.	111

Imagen 34 Repositorio para la descarga de expat.....	111
Imagen 35 Página para la descarga de PCRE.....	112
Imagen 36 Página para la descarga de APR 1.7.4.	113
Imagen 37 Sección para la descarga de APR 1.7.4.	113
Imagen 38 Página para la descarga de APR Util 1.6.3.	114
Imagen 39 Sección para la descarga de APR Util 1.6.3.	114
Imagen 40 Descarga de MySQL Community oficial.	116
Imagen 41 Sección descarga de Zabbix.	118
Imagen 42 Actualización de yum.....	121
Imagen 43 yum actualizado.	122
Imagen 44 Instalación de GCC comprobado.	123
Imagen 45 Cambios en APR-util versión 1.6.0 o superior.	123
Imagen 46 Página para la descarga de expat.	124
Imagen 47 Repositorio para la descarga de expat.....	124
Imagen 48 Descomprimir expat.	124
Imagen 49 Expat descomprimido.....	125
Imagen 50 Configuración en expat.	125
Imagen 51 Comando make en expat.	125
Imagen 52 Comando make install en expat.	125
Imagen 53 Expat instalado.	126
Imagen 54 Página para la descarga de PCRE.	126
Imagen 55 Descomprimiendo pcre2.....	127
Imagen 56 Descomprimiendo pcre2 imagen 2.	127
Imagen 57 Ingresando a la carpeta de pcre2.....	127
Imagen 58 Configuración en carpeta de pcre2.	128
Imagen 59 Configuración en carpeta de pcre2 terminada y comienza comando make.	128
Imagen 60 Comienza comando make install.	128
Imagen 61 Comando make install finalizado.	128
Imagen 62 Página para la descarga de APR 1.7.4.	129
Imagen 63 Sección para la descarga de APR 1.7.4.	129
Imagen 64 Descomprimir apr 1.7.4.	129
Imagen 65 Comando configure en apr 1.7.4.	130
Imagen 66 Comando make en apr 1.7.4.	130
Imagen 67 Comando make install en apr 1.7.4.	130
Imagen 68 Comando make install finalizado en apr 1.7.4.....	130
Imagen 69 Página para la descarga de APR Util 1.6.3.	131
Imagen 70 Sección para la descarga de APR Util 1.6.3.	131
Imagen 71 Descomprimiendo APR Util 1.6.3.	131

Imagen 72 Descomprimiendo APR Util 1.6.3 imagen 2.	132
Imagen 73 Comando configure en APR Util 1.6.3.	132
Imagen 74 Comando make en APR Util 1.6.3.	132
Imagen 75 Comando make install en APR Util 1.6.3.....	133
Imagen 76 Comando make install finalizado en APR Util 1.6.3.	133
Imagen 77 Descomprimiendo httpd.	134
Imagen 78 Comando configure en httpd.	134
Imagen 79 Comando configure finalizado en httpd.	134
Imagen 80 Comando make en httpd.....	135
Imagen 81 Comando make install en httpd.	135
Imagen 82 Descarga de MySQL Community oficial.	135
Imagen 83 Instalación de MySQL Community oficial.	136
Imagen 84 Muestra de la instalación del repositorio MySQL Community oficial.	136
Imagen 85 Instalación de MySQL Community server.	137
Imagen 86 Instalación completa de MySQL Community server.	137
Imagen 87 Ingreso al servidor de MySQL server.	138
Imagen 88 Cambio de contraseña de MySQL server.	138
Imagen 89 Descomprimiendo php 7.3.33.	138
Imagen 90 Comando configure en php 7.3.33.	139
Imagen 91 Comando configure finalizado en php 7.3.33.	139
Imagen 92 Comando make en php 7.3.33.	139
Imagen 93 Comando make install en php 7.3.33.....	140
Imagen 94 Comando make install finalizado en php 7.3.33.	140
Imagen 95 Error e instalación de librería libxml2 para php 7.3.33.	140
Imagen 96 Selección de versión de Zabbix para descargar.	141
Imagen 97 Instalación del repositorio de zabbix.	142
Imagen 98 Instalación del repositorio de zabbix en consola.	142
Imagen 99 Instalación de zabbix server frontend de zabbix en consola.	143
Imagen 100 Creación de base de datos para zabbix en mysql.	143
Imagen 101 Creación de usuario y asignar todos los privilegios para zabbix en mysql.	144
Imagen 102 Set log_bin_trust_function_creators = 1.....	144
Imagen 103 Importando el host de zabbix.	144
Imagen 104 Deshabilitar log_bin_trust_function_creators.....	145
Imagen 105 Dirección /etc/zabbix/zabbix_server.conf para conImagenr base de datos de zabbix.	146
Imagen 106 Dirección /etc/zabbix/zabbix_server.conf para conImagenr base de datos de zabbix imagen 2.	146
Imagen 107 Asignando la contraseña de la base de datos de zabbix en la configuración.	147
Imagen 108 Iniciando el servicio de Zabbix.	148

Imagen 109	Página de inicio de configuración de Zabbix Web.	148
Imagen 110	Página de inicio de configuración de Zabbix Web imagen 2.	149
Imagen 111	Página de inicio de configuración de Zabbix Web imagen 3.	149
Imagen 112	Página de inicio de configuración de Zabbix Web imagen 4.	150
Imagen 113	Página de inicio de configuración de Zabbix Web imagen 5.	150
Imagen 114	Página de inicio de configuración de Zabbix Web imagen 6.	151
Imagen 115	Inicio de sesión de Zabbix Web.	151
Imagen 116	Dashboard por defecto de Zabbix Web.	152
Imagen 117	Puertos servidor y ordenadores conectados en red.	153
Imagen 118	Dirección IP servidor.	153
Imagen 119	Dirección IP ordenador1.	154
Imagen 120	Dirección IP ordenador2.	154
Imagen 121	Ping ordenador 1 a servidor.	155
Imagen 122	Ping ordenador 2 a servidor.	155
Imagen 123	Entrando a zabbix web.	156
Imagen 124	Botón Create host group.	156
Imagen 125	Nombre host group.	157
Imagen 126	Host group added.	157
Imagen 127	Botón Create Host.	157
Imagen 128	Agregando un template ICMP.	158
Imagen 129	Agregando un template ICMP a un host group.	158
Imagen 130	Agregando un agent al host.	159
Imagen 131	Información del host para agregar.	159
Imagen 132	Grafica ICMP ping.	160
Imagen 133	Grafica ICMP response time.	160
Imagen 134	Grafica ICMP los.	161
Imagen 135	Puerto ethernet desconectado ordenador 1.	161
Imagen 136	Puerto ethernet reconectado ordenador 1.	162
Imagen 137	Grafica ICM loss después de reconexión.	162
Imagen 138	Grafica ICM response time después de reconexión.	163
Imagen 139	Creación de host 2 del ordenador 2.	163
Imagen 140	Visualización de agregado del ordenador 2.	164
Imagen 141	Grafica ICMP loss ordenador 2.	164
Imagen 142	Grafica ICMP ping ordenador 2.	165
Imagen 143	Grafica ICMP response time ordenador 2.	165
Imagen 144	Puerto ethernet desconectado del ordenador 2.	166
Imagen 145	Warning de puerto ethernet desconectado del ordenador 2.	166
Imagen 146	Cambio de los datos por la desconexión del puerto ethernet ordenador 2.	167

Imagen 147 Reconexión del puerto ethernet ordenador 2.	167
Imagen 148 Warning de problema resuelto de puerto ethernet ordenador 2.	168
Imagen 149 Cambio de información por solvencia de problema de puerto ethernet ordenador 2.	168
Imagen 150 Cambio en la gráfica ICMP loss ordenador 2.	169
Imagen 151 Cambio en la gráfica ICMP ping ordenador 2.	169
Imagen 152 Cambio en la gráfica ICMP response time ordenador 2.	170
Imagen 153 Puertos de servidor y ordenador de prueba conectados.	173
Imagen 154 Dirección IP asignada a ordenador de prueba.	173
Imagen 155 Dirección IP asignada a servidor.	174
Imagen 156 Ping de ordenador de prueba a servidor.	174
Imagen 157 Ping de servidor a ordenador de prueba.	175
Imagen 158 Descarga del agente Zabbix para Windows.	175
Imagen 159 Descarga del agente Zabbix para Windows versión 6.0.19.	176
Imagen 160 Configuración de agente Zabbix por asistente para Windows.	177
Imagen 161 Instalar Agente Zabbix en Windows.	177
Imagen 162 Agente Zabbix instalado en Windows.	178
Imagen 163 Selección de ordenador.	179
Imagen 164 Selección de configuración.....	179
Imagen 165 Selección de botón template select para elegir plantilla.....	180
Imagen 166 Selección de plantilla host group template.	180
Imagen 167 Selección de Windows by Zabbix Agente template.	181
Imagen 168 Agregar un agente para la plantilla seleccionada.	181
Imagen 169 Lastest data del servidor de prueba para ver los datos recolectados.	182
Imagen 170 Lastest data del servidor de prueba para ver los datos recolectados imagen 2.	182
Imagen 171 Lastest data del servidor de prueba para ver los datos recolectados imagen 3.	183
Imagen 172 Gráfica CPU user time de ordenador de prueba.....	183
Imagen 173 Columna Graph de ordenador de prueba.	184
Imagen 174 Grafica general de CPU usage y CPU utilization de ordenador de prueba.	184
Imagen 175 Desconexión de ethernet de ordenador de prueba.	185
Imagen 176 Cambios en las gráficas de ICMP loss y ping de ordenador de prueba.	185
Imagen 177 Cambios en las gráficas de ICMP response time de ordenador de prueba.	186
Imagen 178 Opción Problems en ordenador de prueba para visualizar los incidentes.	186
Imagen 179 Problems en ordenador de prueba para visualizar los incidentes.	187
Imagen 180 Ventana de actualización del problema presentado en ordenador de prueba.	187
Imagen 181 Cambios realizados al incidente.	188
Imagen 182 Información sobre el incidente de ordenador prueba.	188
Imagen 183 Resolución de un incidente después de la reconexión de ethernet en ordenador de prueba.	188

Imagen 184 Resolución de todos los incidentes después de la reconexión de ethernet en ordenador de prueba.	188
Imagen 185 Opción de administrar mi cuenta de Google.	189
Imagen 186 Opción de verificación en 2 pasos.	189
Imagen 187 Llenado de información necesario de verificación en 2 pasos.	190
Imagen 188 Creación de una contraseña para aplicaciones.	190
Imagen 189 Creación de una contraseña para Zabbix.	191
Imagen 190 Contraseña generada para el envío de correos por Zabbix.	191
Imagen 191 Configuración de email en zabbix.	192
Imagen 192 Configuración de email en zabbix en media types.	192
Imagen 193 Configuración de acciones de triggers en Configuration.	193
Imagen 194 Configuración de acciones de triggers en new conditions.	193
Imagen 195 Configuración de acciones de triggers en Operation details.	194
Imagen 196 Configuración de user profile del administrador del usuario zabbix.	194
Imagen 197 Configuración de user profile del administrador del usuario zabbix en pestaña Media.	195
Imagen 198 Envío de prueba de correo electrónico de advertencia de evento de Zabbix.	195
Imagen 199 Email conImagendo y desplegado en acciones de un problema en zabbix.	196
Imagen 200 Correo de prueba y de notificación de error en Gmail.	196

TESCo

ÍNDICE DE TABLAS

Tabla 1 Análisis FODA por miembros del departamento de TIC's.	50
Tabla 1 Análisis FODA por miembros del departamento de TIC's.(Continuación)	51
Tabla 2 Análisis FODA por usuarios de los departamentos dependientes de TIC's	51
Tabla 2 Análisis FODA por usuarios de los departamentos dependientes de TIC's (Continuación). ...	52
Tabla 3 Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.	52
Tabla 3 Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.(Continuación 1)	53
Tabla 3 Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.(Continuación 2)	54
Tabla 3 Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.(Continuación 3)	55
Tabla 4 Indicadores de riesgo y prioridad de atención.	58
Tabla 4 Indicadores de riesgo y prioridad de atención. (Continuación).	59
Tabla 5 Indicador de ocurrencia.	59
Tabla 6 Indicador de impacto.	59
Tabla 7 Valoración de riesgo de acuerdo a impacto y ocurrencia.	60
Tabla 8 Matriz de prioridad de atención de acuerdo a impacto y ocurrencia.....	60
Tabla 9 Tabla de prioridad de atención de acuerdo a impacto y ocurrencia.	60
Tabla 4 Indicadores de riesgo y prioridad de atención.(Continuación).	61
Tabla 10 Tabla de valoración de riesgo por el personal de TIC's.	61
Tabla 10 Tabla de valoración de riesgo por el personal de TIC's.(Continuación 1)	62
Tabla 10 Tabla de valoración de riesgo por el personal de TIC's.(Continuación 2)	63
Tabla 11 Tabla de valoración de riesgo por los usuarios de departamentos.	64
Tabla 11 Tabla de valoración de riesgo por los usuarios de departamentos. (Continuación),	65
Tabla 12 Tabla síntesis del análisis de riesgos.	66
Tabla 12 Tabla síntesis del análisis de riesgos. (Continuación).....	67
Tabla 13 Relación Vulnerabilidad/Amenaza.	68
Tabla 13 Relación Vulnerabilidad/Amenaza, (Continuación).	69
Tabla 14 Recomendaciones para vulnerabilidades relacionadas a la poca eficiencia en TIC's.	71
Tabla 14 Recomendaciones para vulnerabilidades relacionadas a la poca eficiencia en TIC's, (Continuación),	72
Tabla 15 Matriz relación entre miembros, indicadores y actividades a realizar para tratar las vulnerabilidades relacionadas a la poca eficiencia en TIC's.	73
Tabla 16 Recomendaciones para vulnerabilidad relacionada al ancho de banda.	77
Tabla 16 Recomendaciones para vulnerabilidad relacionada al ancho de banda. (Continuación)	78

Tabla 17 Estrategias resultantes de la relación vulnerabilidad/amenaza.	78
Tabla 18 Matriz relación entre miembros, indicadores y actividades a realizar para tratar las vulnerabilidades relacionadas a la educación y concientización de los usuarios.	80
Tabla 19 Recomendaciones para vulnerabilidad relacionada al monitoreo en la red.	82
Tabla 20 Estrategias resultantes de la relación vulnerabilidad/amenaza para el monitoreo de red.	83
Tabla 21 Métrica de evaluación para herramienta de software.	84
Tabla 22 Ventajas/desventajas de wireshark.	88
Tabla 23 Métrica de evaluación para WireShark.	90
Tabla 24 Resumen características de Zabbix.	91
Tabla 25 Métrica de evaluación para Zabbix.	96
Tabla 26 Tabla comparativa entre PRTG, Zabbix y WireShark.	99
Tabla 27 Pre requisitos en software para zabbix.	101
Tabla 28 Pre requisitos en hardware para zabbix y hardware proporcionado.	102
Tabla 29 Requisitos para compilar Apache.	109
Tabla 30 Formas de instalar GCC.	109
Tabla 31 Maneras de instalar PHP.	115
Tabla 32 Hardware proporcionado por la empresa.	120
Tabla 33 Maneras de instalar GCC.	122
Tabla 34 Maneras de instalar PHP.	133
Tabla 35 Información a monitorear para prueba de agentes.	172

TESCo

INTRODUCCIÓN

La Comisión Federal de Electricidad (CFE), es una empresa pública de carácter social que provee energía eléctrica. Es una empresa productiva del Estado, propiedad exclusiva del gobierno federal, con personalidad jurídica y patrimonio propio.

Actualmente, la zona Cuautitlán CFE, ha tenido algunas necesidades para mejorar la operatividad y seguridad sobre todo de sus servicios de redes, al realizar los análisis basados en cuestionarios, FODAS, riesgos y ayuda de la norma ISO-IEC 27001:2013, se obtuvieron las vulnerabilidades, de gran o bajo riesgo, cuales la empresa debe prestar atención, principalmente vulnerabilidades relacionadas a posibles ataques/mal uso de los recursos y el poco personal de TICs asignado al departamento. Con el fin de dar solución o provenir que las vulnerabilidades sean explotadas se propusieron recomendaciones y estrategias basados en la norma ISO-IEC 27001:2013 y el marco de trabajo COBIT 4.0. De entre todas estas estrategias, de acuerdo a los requerimientos de la empresa y sus necesidades, se ha trabajado en la investigación, la instalación, configuración e implementación de un servidor en CentOS para la herramienta de monitoreo de Zabbix en CFE zona Cuautitlán, con el objetivo de un mayor control en la intranet.

Para la implementación del servidor se investigó la forma de instalación y pre-requisitos de fuentes oficiales como lo son CentOS.org, Red Hat, Apache, MySQL, entre otros, además de pruebas de instalación, pruebas de uso de Zabbix y recomendaciones. Los requerimientos de la empresa marcan un avance o no en la escalabilidad.

Zabbix es una herramienta con gran potencial para tratarse de un software sin licencia de paga, que como se propuso en las recomendaciones finales, con ayuda de los agentes de Zabbix, sencillos de instalar en ordenadores Windows, sistema operativo designado para los usuarios en la intranet de CFE, se puede obtener información del sistema y hardware sin necesidad de la complejidad y posibles vulnerabilidades que puede generar el protocolo SNMP.



TESCo

CAPÍTULO I GENERALIDADES DEL PROYECTO

El siguiente capítulo expone la problemática, justificación, objetivos y otros elementos que conforman la introducción al tema a desarrollar y parte del protocolo.

TESCO

DESCRIPCIÓN DE LA EMPRESA

Nombre; Comisión Federal de Electricidad

Razón social; Comisión Federal de Electricidad

Lugar; Zona Cuautitlán Izcalli

Organigrama

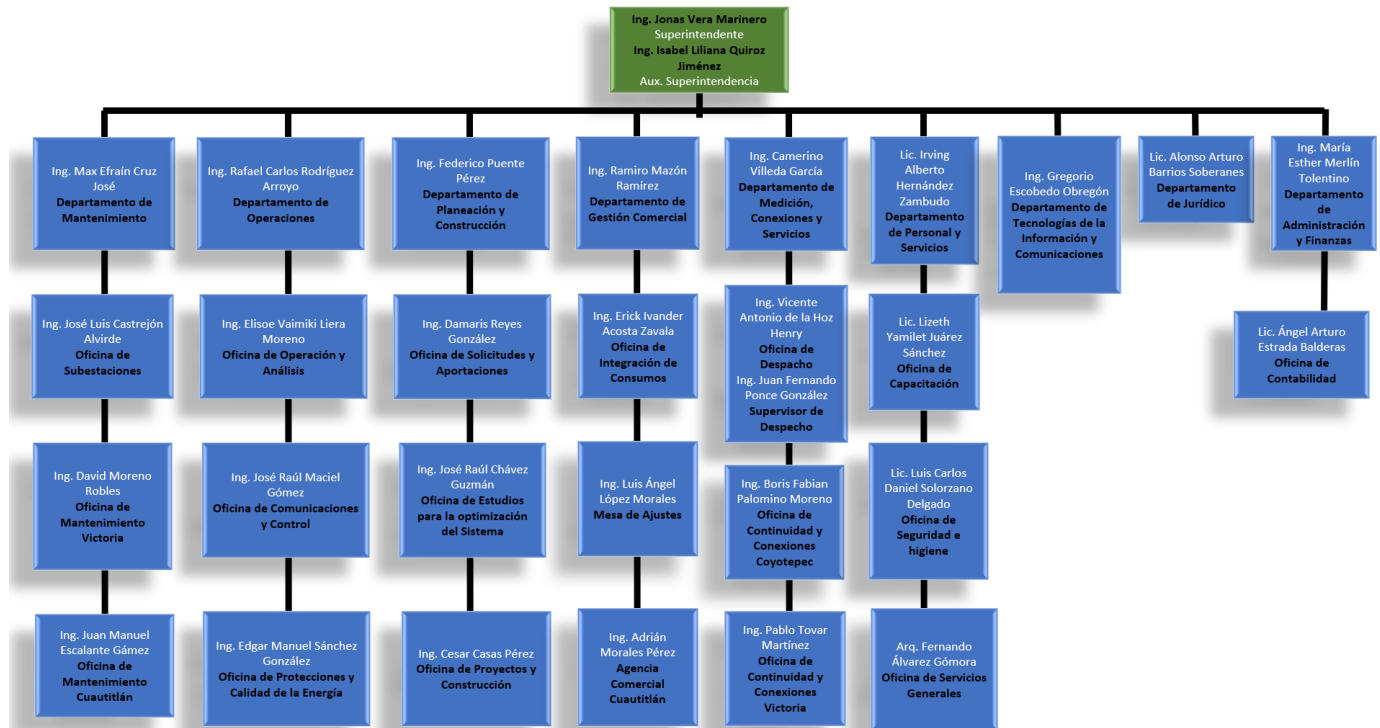


Imagen 1 Organigrama general de CFE Zona Cuautitlán, imagen1. [Fuente Propia]

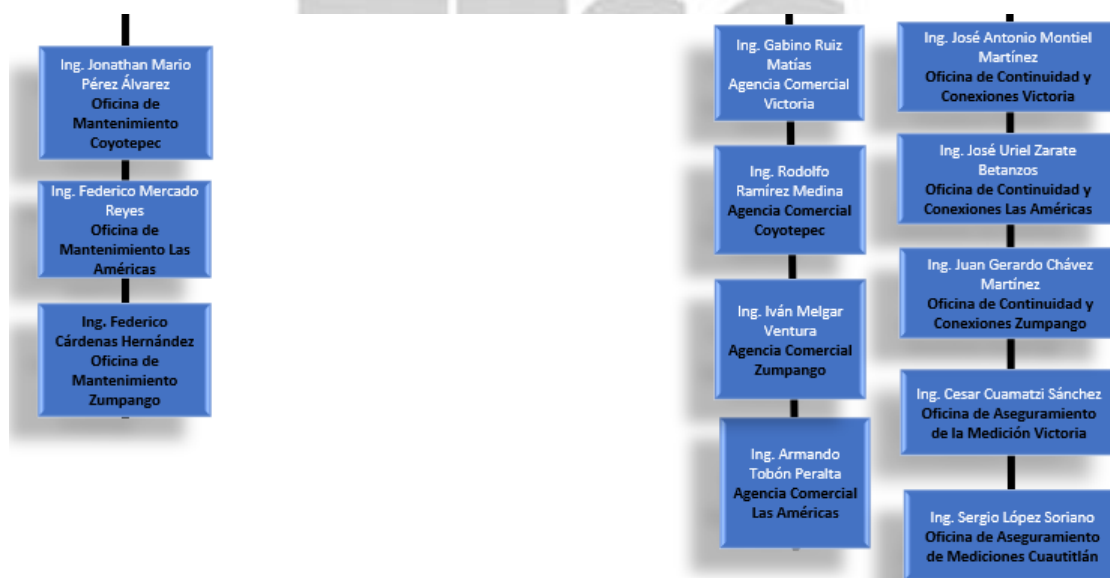


Imagen 2 Organigrama general de CFE Zona Cuautitlán, imagen2. [Fuente Propia].

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

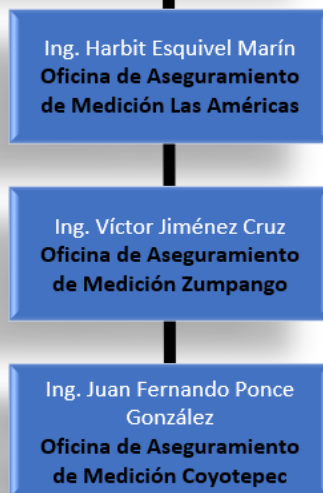


Imagen 3 Organigrama general de CFE Zona Cuautitlán, imagen3. [Fuente Propia].



Imagen 4 Organigrama general de CFE Zona Cuautitlán, imagen4. [Fuente Propia].

Nota: Por parte de las residencias profesionales, me encuentro dentro del departamento de mi asesor interno siendo “Departamento de Tecnologías de la Información y Comunicaciones”.

Sector productivo de la empresa; Red de distribución de energía eléctrica

Misión

Suministrar insumos y bienes energéticos requeridos para el desarrollo productivo y social del país de forma eficiente, sustentable, económica e incluyente, mediante una política que priorice la seguridad y la soberanía energética nacional y fortalezca el servicio público de electricidad. [Comisión Federal de Electricidad, s.f.]

Visión

Consolidarnos como la empresa de energía líder en México, con solvencia técnica y financiera, que procura el fortalecimiento de nuestro capital humano y garantiza el servicio de energía eléctrica con calidad y sentido social a nuestros clientes en todos los segmentos del mercado, para contribuir al desarrollo sustentable del país, generando valor económico y rentabilidad al Estado Mexicano. [[Comisión Federal de Electricidad, s.f.](#)]

Filosofía y/o Valores

Todos quienes integran la Comisión Federal de Electricidad deben y deberán actuar y conducirse en base a los principios de transparencia, honestidad, eficiencia, equidad y responsabilidad social, además de adquirir y demostrar los valores institucionales de Integridad, Productividad y Responsabilidad. [[Comisión Federal de Electricidad, 27 de abril de 2022, pág. 9 – 16](#)].

Breve historia de la empresa.

Hasta 1937 en México existían tres compañías proveedoras de electricidad; The Mexican Light and Power Company, The American and Foreign Power Company, y la Compañía Eléctrica de Chapala, cuyos servicios tenían tarifas elevadas y constantes interrupciones de energía. En este mismo año el gobierno federal creó el 14 de agosto a la Comisión Federal de Electricidad, con objetivo de distribuir la energía a nivel nacional, sin fines de lucro, reducir los costos y aumentar el rendimiento económico.

En 2009, la CFE es la encargada de brindar el servicio eléctrico a toda la república mexicana. En el 2016 se dividió a la CFE en 9 empresas subsidiarias y 4 filiales.

Actualmente CFE opera en todo el país organizado en cuatro procesos; generación, transmisión, distribución y suministrador. [[Comisión Federal de Electricidad, s.f.](#)]

PROBLEMA A RESOLVER

La CFE es una empresa de nivel mundial cuyo objetivo principal es brindar servicio de energía eléctrica a la población mexicana, encargándose de la generación, transmisión, distribución y suministro de la energía a los hogares, negocios e industrias.

El Departamento de Tecnologías de la Información y Comunicaciones en la Zona Cuautitlán, se encarga de la administración e implementación de sistemas informáticos, además de brindar soporte técnico y opera bajo las políticas que rigen las TIC dentro de CFE obtenidas del documento con nombre "Políticas de Tecnologías de la Información, Comunicaciones y Seguridad de la Información de la Comisión Federal de Electricidad, Empresas Productivas Subsidiarias y, en su caso, Empresas Filiales.", con fecha 20 de diciembre de 2022.

El proceso que más escalabilidad y atención requiere es el de monitorear la intranet de la Zona Cuautitlán en CFE Cuautitlán Izcalli localmente.

Los procesos de monitoreo de la red local no se encuentran aplicados. El departamento de TIC cuenta con un inventario de equipos de cómputo, direcciones IP, de switches, routers, entre otros, sin embargo, no se conoce que equipos generan picos de ancho de banda y el por qué, tampoco. Hacia donde se envía ping por parte de los equipos es desconocida. Esta situación puede generar una brecha de seguridad, al pasar desapercibido estos dos aspectos relacionados con los protocolos ICMP y SNMP, se puede generar un ataque de denegación de servicios o el mal uso de los recursos en la red. Igualmente, es conocido que existen oportunidades en estos aspectos porque se ha visto en el mundo y documentado en artículos e informes académicos como por pasar por alto que un puerto este abierto, llegase a entrar un ataque enfocado a infiltraciones o robo de información (Universidad del Cauca. (2006). Utilizando Inteligencia Artificial para la detección de puertos), o que uno de los más comunes errores en las redes IP, nuevamente, son el inadecuado uso del ancho de banda, así como su configuración y ajuste (Eusebi Calle. Universidad de Girona. (s.f.). Arquitectura del Sistema de Gestión del ancho de Banda y Protección (SGBP) para entornos de redes MPLS).

El problema que enfrenta localmente la organización es el desconocimiento de las actividades de los usuarios en la red, en donde se generan grandes picos de ancho de banda, que puertos están siendo usados. La organización necesitara documentación de estos, es un área de oportunidad, si bien cuenta con políticas a nivel nacional, no cuenta con documentación de procesos que se trabajan en las oficinas del área local. Las consecuencias podrían impactar

negativamente la seguridad en la intranet, ya que un mayor tráfico en el ancho de banda desencadena el bajo rendimiento que tendrán las conexiones de los usuarios en la red, el no tener control sobre los puertos y que tipo de información es compartida, puede dar lugar a la transferencia de archivos basura, innecesarios, malware o provocar acciones mal intencionadas.



TESCO

OBJETIVOS

Objetivo general

Implementar un Servidor CentOS con norma ISO-IEC 27001:2013 para seguridad de Intranet de CFE Zona Cuautitlán

Objetivos específicos

1. Evaluar el área de TIC'S , enfocándose en el proceso actual de operación de monitoreo de las redes de intranet de Zona Cuautitlán.

1.1 Realizar entrevista para conocer a la organización de forma general (contexto, políticas, infraestructura), la situación y si existen controles por parte del departamento de TIC de Zona Cuautitlán.

1.2 Realizar una entrevista sobre el área problemática en monitoreo de redes de la zona Cuautitlán

1.3 Realizar cuestionarios a usuarios de 4 diferentes departamentos sobre el departamento de TICs.

2. Diagnosticar el área de TIC'S, enfocándose en el proceso actual de operación de monitoreo de las redes de intranet de Zona Cuautitlán.

2.1 Diagnostica con un análisis de Fortaleza, Oportunidades, Amenazas y Debilidades del departamento de TIC de Zona.

2.2 Diagnosticar con un análisis de riesgos sobre la situación actual del área problemática a apoyar

2.3 Genera informe que integre amenazas y vulnerabilidades de área de TIC y monitoreo de redes, así como las posibles estrategias de seguridad.

3. Implementar medidas de seguridad: Servidor CentOS con norma ISO-IEC 27001:2013 para seguridad de Intranet de CFE Zona Cuautitlán

3.1 Evaluar herramientas y tecnologías para la implementación del servidor

3.2 Definir la configuración del servidor y de zabbix para su instalación

3.3 Implementar el servidor en la red local

3.4 Realizar recomendaciones de uso de agentes para monitoreo de la red

JUSTIFICACIÓN

El Departamento de Tecnologías de la Información y Comunicaciones en la Zona Cuautitlán, se encarga de la administración e implementación de sistemas informáticos, además de brindar soporte técnico. Debido a esto, cuenta con inventarios para los equipos de cómputo y dispositivos de red, sin embargo, no cuenta con toda la documentación del estatus de sus equipos ni monitoreo localmente de los mismos que son asignados a los usuarios. Ello puede perjudicar a los procesos y actividades dentro de la empresa, si un usuario no está utilizando correctamente los recursos de la red o que pudiese existir brechas de seguridad, por lo que son de importancia enfocarse en los protocolos ICMP y SNMP para monitoreo de los equipos.

El identificar debilidades u oportunidades en la empresa, así mismo los riesgos y tomar las medidas de prevención y aplicarlas, ayudando al departamento a cargo de las tecnologías de la información es una tarea que requiere de tiempo y esfuerzo, y que en este momento a través de la realización de este proyecto se podrá evaluar y conocer la infraestructura de la empresa y generar estrategias basadas en la norma ISO-IEC 27001:2013 enfocada en Seguridad de la Información a fin de mejorar su entorno de aseguramiento.

Los beneficios de superar estos inconvenientes van más allá de la identificación, ya que incluye el asegurar razonablemente la integridad, disponibilidad y confiabilidad de la información, con ello trae mejores prácticas de seguridad y mejora continua, ya que al tratarse esta brecha en la intranet de Zona Cuautitlán un asunto que involucra protocolos tan útiles como el ICMP y SNMP, da a lugar a la futura administración de los equipos informáticos con la implantación de mejores controles.

Con ayuda de la aplicación de la norma ISO-IEC 27001:2013 al proceso de evaluación en la organización se puede identificar las amenazas, los riesgos, las áreas donde estén las posibles brechas de seguridad y formular estrategias que ayuden a monitorear la intranet local de la zona Cuautitlán Izcalli para CFE.

Añadiendo que, de comenzar a usar buenas prácticas de seguridad basado en esta norma, brinda una mejor imagen de la organización, tanto para clientes, proveedores y auditores, posteriormente podría incluso llevar a la certificación de la organización.

CAPÍTULO II

MARCO TEÓRICO

El siguiente capítulo se encuentra dividido en tres partes y expone la historia, fundamentos y conceptos, así como la serie de pasos para la realización de este proyecto.

TESCO

Marco Histórico - Contextual

El desarrollo de los servidores ha sido un gran avance y evolución para las áreas de la informática y las comunicaciones. Desde sistemas aislados para compartir recursos en redes locales o en intranets, hasta complejas infraestructuras de nubes que proveen de servicios a compañías y sistemas alrededor del mundo. Es así, los servidores constantemente han avanzado tecnológicamente impulsados por las necesidades de procesamiento, almacenamiento, transmisión o distribución de datos.

Entre las décadas de 1940 y 1950, los primeros servidores surgieron como máquinas compuestas de tubos de vacío y relés electromecánicos, operando con temperaturas frías, datos básicos y operaciones complejas. Fue hasta la década de 1950 cuando surgen los conceptos de servidores en forma de mainframes, cuyos sistemas eran capaces de procesar y almacenar volúmenes de datos a través de terminales remotas.

Después entre 1960 y 1970 el surgimiento de mainframes los hizo posicionarse en la infraestructura computacional empresarial, gestionando principalmente procesos de nóminas e inventarios.

Para 1980 y 1990 con la aparición de las redes de computadoras, dio una gran evolución a los servidores en la red. Estos dispositivos permitían compartir recursos, datos, y en poco tiempo se convirtieron en una pieza clave e inseparable de la informática en red. Más tarde con la expansión y auge del internet, los servidores siempre estaban presentes en la World Wide Web, con ello compañías que nacieron sobre servidores como HTTP Apache y Microsoft impulsaron más el uso de los servidores, su contenido que pudiesen almacenar y compartir en la internet y surgieron de esta manera el comercio electrónico.

Más tarde en los años 2000, la virtualización se implementó en los servidores. Tecnologías de virtualización permitieron la creación de máquinas virtuales, varias de ellas en un solo servidor físico, optimizando recursos y dando paso a la escalabilidad.

En la actualidad los servidores se han mejorado en almacenamiento, velocidad y capaces de realizar varios procesos, ofreciendo además de recursos, también servicios, en breve el concepto de la nube, siendo servidores que almacenan grandes cantidades de información,

proveedores de ella y de servicios digitales, contribuyen a una gran parte de la infraestructura económica y social actual. [\[Ceruzzi, P.E., 2017\]](#), [\[Gromala, D., 2019\]](#), [\[Freeman, J., 2015\]](#)

Marco Conceptual

Agentes

Son parte de un software, entonces los agentes son software programados para ser parte de un ambiente (el entorno donde realizaran sus acciones O tareas para lo que fueron programados), sensor su entorno (son capaces de “percibir” algunas acciones características de su ambiente) y dependiendo de esto actuar para realizar alguna tarea, recopilando datos, desencadenando alguna acción, comenzar un proceso, entre otras.

En Zabbix existen dos tipos de agentes: Zabbix agent (ligero, multiplataforma, escrito en C) y Zabbix agent 2 (flexible, puede ampliarse con plugins, escrito en Go). [\(Zabbix, s.f.\)](#)

Ancho de banda

Es referenciado para definir la cantidad de datos que pueden ser enviados a través de una red o circuito de comunicación en un tiempo estimado, normalmente en bits por segundos.

Esta propiedad tiene relación con la velocidad de transmisión de datos. [\(Universidad Nacional Autónoma de México, s.f.\)](#)

Asíncrono (redes)

Se refiere a transmisión de datos (o actividades en un contexto más general) que pueden realizarse más de uno de estos procesos a la vez y que no sigue un patrón regular en el tiempo de transferencia.

Un ejemplo de esta característica es cuando se envía datos a un servidor. Varios equipos informáticos piden peticiones durante cualquier tiempo, a una hora cualquiera, cuantas veces se desee, recibiendo información en diferentes intervalos de tiempo. [\(Mozilla, s.f.\)](#)

CentOS

Definición

Es un sistema operativo Linux creado por contribuciones que hace la misma comunidad de

Linux, de esta manera generando una nueva distribución.

Funcionalidad

Es un sistema mayormente enfocado a servidores, proveedores de servicios de nube, hosting y procesamiento de datos científicos. ([Red Hat, 2021](#)), ([CentOS, s.f.](#))

Capa 2 – 3

La capa 2 es la capa de vínculo de datos, segundo nivel del modelo OSI de siete capas o la última capa baja de TCP/IP. Esta capa es utilizada para transferir datos entre nodos de red adyacentes (nodos vecinos o existe conexión entre ellos). Los switches capa dos permiten la transmisión de datos entre equipos haciendo uso de la dirección MAC del equipo emisor al receptor.

La capa 3 es la capa de red. Los switches de capa 3 pueden transmitir los datos como los switches de capa 2 y además transmitirlos no solo por MAC, también por dirección IP, y trazar la mejor ruta para la transmisión. ([HUAWEI, 2022](#))

CD (CFE)

Centro de distribución, son agencias donde se centra personal el personal operativo en sus diferentes áreas, por ejemplo, medición, administración, distribuciones, entre otros, y se llevan a cabo los diferentes procesos y actividades para que la empresa funcione. [[J. Williams, 2023](#)]

Distribución (Sistemas Operativos)

Son versiones de sistemas operativos creadas o modificadas que aporta cada comunidad o proveedor a partir de un sistema operativo base. ([Red Hat, 2023](#))

División (CFE)

Hay 16 divisiones existentes en CFE, la división donde esta Cuautitlán es la división valle de México norte, dentro de ella hay 7 zonas, cada división tiene una gerencia que,

cada zona se divide en centros de distribución. ([J. Williams, 2023](#))

DownStream & UpStream

Hablando especialmente de los sistemas operativos de Red Hat y CentOS, un sistema upstream sería una versión preliminar a un sistema operativo, el cual se mejorará o aportaran herramientas. Luego este sistema al liberarse y de él crear uno o basarse en su código, surge el sistema downstream.

Por ejemplo, como es el caso de CentOS 8 Stream, es una versión donde la comunidad aporta mejoras o características para posteriormente convertirse en Red Hat Enterprise Linux 8. DownStream haría referencia a CentOS Linux 8, ya que después con el código resultante de Red Hat Enterprise Linux 8 se crearía esta versión de CentOS. ([CentOS, s.f.](#))

Enlaces (CFE)

Es un vínculo que existe entre equipos informáticos o medios digitales, que usan una interfaz de conexión ya sea el cableado o señales para el caso de medios físicos, o direcciones y señales para medios digitales. ([J.Williams, 2023](#))

ICMP (protocolo de control de mensajes de internet)

Es un protocolo usado en los dispositivos de red para el diagnóstico de problema de comunicación. Este protocolo se encuentra en la capa de red.

Su principal utilidad es el informar de errores existentes en los envíos de datos, cuáles pueden ser las posibles fuentes de retraso en la red, si llegan a su destino o no, realizando pruebas de ping y traceroute. Además de estos beneficios, también puede ser utilizado para generar ataques de denegación de servicios.

Sobre sus dos principales utilidades, el tracerouter, indica cuantos saltos o la trayectoria en los routers por los que ha pasado la información hasta llegar al destino, y en cuanto al ping, muestra el tiempo al que tardó en llegar a su destino los paquetes de información. ([CloudFlare, s.f.](#))

Intranet

Es una red interna a la empresa u organización donde se comparte información, funciones, servicios y recursos, usando una infraestructura similar a la red internet, quiere decir, uso de servidores y protocolos, este tipo de red restringe el acceso a solo usuarios autorizados para mantener la seguridad de información a redes exteriores. Puede estar totalmente aislada o conectada a internet u otras redes, pero limita la información entrante y saliente.

Protocolos normalmente usados en una intranet:

FTP (File Transfer Protocol)

Es un protocolo que permite la transferencia de archivos entre computadores y servidores, incluso si son de diferentes sistemas operativos o diferentes formatos de almacenamiento.

Telnet

Es un protocolo para realizar una conexión remota entre computadoras y/o servidores, no es segura totalmente y debe complementarse con otros protocolos como SSH para encriptar la información.

Para que funcione, debe de mantenerse abierto el puerto 23 en la máquina destino y habilitada para tener acceso.

TCP/IP

Ventajas de las Intranets

- a) Contacto directo entre los usuarios pertenecientes a la organización
- b) Fácil publicación, modificación y transferencia de información interna
- c) Al ser aislada o limitada a la internet, descarta, evade y elimina información innecesaria y poco confiable ajena a la organización
- d) La información es utilizada y creada bajo la cultura organizativa
- e) Mayor control y conocimiento de lo que ocurre con las actividades de los usuarios, monitoreando sus actividades, previniendo amenazas

(José T., s.f.)

Máquina Virtual

Es un entorno virtual que permite funcionar un sistema informático dentro de un equipo físico, compartiendo el hardware para el sistema en el equipo y la o las máquinas virtuales. De tal manera que es similar a tener varios ordenadores dentro de uno: Existen limitaciones de recursos compartidos, ya que podría afectar el rendimiento del sistema principal. ([Red Hat, 2023](#))

MIB

Son base de datos que contienen información de las propiedades de un dispositivo para ser administrados por protocolo SNMP para obtención o manipulación de datos.

([Oracle. S.f.](#))

NAT

Es un protocolo que convierte las direcciones IP de una red en una sola dirección IP pública para conectarse a redes externas. Quiere decir que por ejemplo si existen 5 dispositivos en una red, con IP 192.168.0.1, al .0.5, para enviar información a la internet, NAT convertirá esas 5 diferentes direcciones IP a una sola como por ejemplo 10.0.0.1, dirección que representa las 5 anteriores.

NAT en máquinas virtuales tiene la función de cambiar la IP de la máquina física por otra distinta para ser asignada a la máquina virtual, de lo contrario, causaría conflicto por que indicaría que existen en la misma red dos dispositivos con la misma dirección IP interna. ([CISCO, s.f.](#))

Ítems

Es la unidad básica de recolección de datos en Zabbix. Sin ítems la obtención de cualquier dato de un dispositivo no es posible.

([Zabbix, s.f.](#))

Open Source

Es software cuyo código fuente es accesible al público para ser modificado, suele ser flexible, gratuito, durabilidad y complejidad dependientes de la comunidad o autor que lo desarrolle o complemente.

GitHub es un repositorio donde muchos proyectos open source son guardados para ser descargados. ([Red Hat, 2023](#))

Sensor (PRTG)

Son herramientas con las cuales se monitorea un dispositivo, entre ellos el tráfico de un puerto de switch, carga de la CPU de un servidor o el espacio libre de los discos duros. Es recomendable el uso de 5 a 10 sensores por dispositivo, o el uso de un solo sensor para cada puerto switch.

Función general

Los sensores se usan para representar un dispositivo real, físico o funcionalidad de un equipo, por ejemplo, dentro del software creamos y asignamos un dispositivo para representar el firewall, otro para la impresora, en cada dispositivo se puede agregar uno o más sensores. Cada sensor monitorea un aspecto de los dispositivos, por ejemplo, la carga de una cpu en un servidor, el tráfico de red, el ping, el estado del toner, etc. (PAESSLER, s.f.)

SNMP

Protocolo para la administración de transferencia de información en redes, especialmente orientado a las redes LAN.

Con este protocolo se obtiene información, extrayéndola de los dispositivos conectados a una red, así mismo, también puede configurar funciones de los dispositivos.

Algunas características son:

- *Este protocolo es de capa 7 (capa de aplicación)
- *utiliza el puerto 161 para enviar mensajes
- *Los mensajes recibidos por el puerto 162 normalmente son trampas

Tipos de mensajes SNMP:

*GetRequest: se trata del mensaje que envía un administrador SNMP para solicitar datos. El dispositivo objetivo devuelve el valor solicitado con un mensaje de respuesta.

*GetNextRequest: el administrador de SNMP puede enviar este tipo de mensaje para descubrir qué información está disponible desde el dispositivo. Los usuarios pueden

descubrir todos los datos disponibles en un determinado dispositivo.

*GetBulkRequest: aparece por primera vez en SNMP 2, y se trata de una versión más nueva y optimizada de GetNextRequest. La respuesta solicitada contendrá tantos datos como permita la solicitud.

*SetRequest: comando para establecer o modificar el valor de un parámetro a través de SNMP en el dispositivo o sistema del agente. Este tipo de mensaje se puede usar para administrar o actualizar la configuración u otros ajustes. Un SetRequest incorrecto podría afectar seriamente a los sistemas y las configuraciones de red.

*Response: mensaje que un agente de dispositivo envía tras una solicitud del administrador. GetRequest, el paquete contiene los datos o valores solicitados. SetRequest, el paquete responde indicando el nuevo valor establecido a modo de confirmación de que el SetRequest se ha completado con éxito.

*Trap(v2): el agente SNMP envía (“expulsa”) una trampa sin que el administrador lo haya solicitado. De hecho, las trampas se envían bajo determinadas condiciones, como en caso de un error o al sobrepasar un umbral preestablecido. Las trampas son una excelente idea en términos de supervisión proactiva, pero si los usuarios desean beneficiarse de su uso, es posible que primero tengan que configurarlas con la ayuda del administrador de SNMP.

*InformRequest: este tipo de mensaje se agregó en SNMP v2 para dar al administrador la posibilidad de confirmar que ha recibido un mensaje de captura de un agente. Algunos agentes están configurados de modo que sigan enviando una trampa hasta recibir la confirmación de un mensaje de informe.

*Report: los mensajes Report necesitan SNMP v3 y permiten que un administrador de SNMP determine qué tipo de problema detectó el agente SNMP remoto. Dependiendo del error detectado, el motor de SNMP puede intentar enviar un mensaje corregido.

([PAESSLER, s.f.](#))

Servidor

Son ordenadores que provee de recursos, datos, servicios o programas a los ordenadores, también conocidos como clientes, a través de una red. ([PAESSLER, s.f.](#))

Template

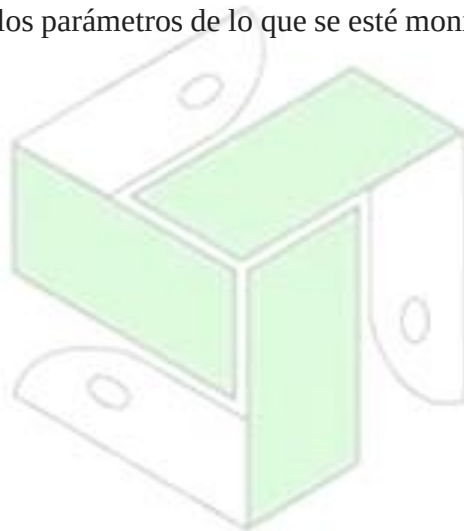
Las plantillas son un conjunto de ítems, triggers y otros elementos reunidos por defecto para monitorear un conjunto de aspectos e información de un ordenador a zabbix.

([ZABBIX, s.f.](#))

Zabbix

Es un software gratuito de código abierto para monitorear variedad de parámetros de las redes, estado e integridad de los servidores, máquinas virtuales, base de datos, servicios, aplicaciones, sitios web, entre otros.

Zabbix usa notificaciones vía e-mail para alertar sobre algún cambio o anomalía, ofrece reportes y estadísticas sobre los parámetros de lo que se esté monitoreando. ([ZABBIX, s.f.](#))



TESCO

Marco Metodológico

Las actividades desarrolladas y utilizadas para la realización del proyecto están acorde a los objetivos específicos para la obtención e investigación de información, uso de las normas y técnicas para finalmente lograr la implementación, estrategias y recomendaciones del proyecto actual y soluciones futuras.

Calendario																															
		Mes/Semana																													
				Abril					Mayo					Junio					Julio					Agosto							
		Objetivo		Actividad		S2	S3	S4	S5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5		
O b j e t i v o s E s p e	1) Evaluar el área de TIC'S, enfocándose en el proceso actual de operación de monitoreo de las redes de intranet de Zona Cuautitlán.	1.1 Realizar entrevista para conocer a la organización de forma general (contexto, políticas, infraestructura), la situación y si existen controles por parte del departamento de TIC de Zona Cuautitlán.																													
		1.2 Realizar una entrevista sobre el área problemática en monitoreo de redes de la zona Cuautitlán																													
		1.3 Realizar cuestionarios a usuarios de 4 diferentes departamentos sobre el departamento de TICs.																													
	2) Diagnosticar el área de TIC'S, enfocándose en el proceso actual de operación de monitoreo de las	2.1 Diagnostica con un análisis de Fortaleza, Oportunidades, Amenazas y Debilidades del departamento de TIC de Zona.																													
		2.2 Diagnosticar con un análisis de riesgos sobre la situación actual del área problemática a apoyar																													

Imagen 5 Calendario de actividades en base al objetivo específico durante la Residencia Profesional. [Fuente Propia].

P e c i f i c o s	redes de intranet de Zona Cuautitlán.	2.3 Genera informe que integre amenazas y vulnerabilidades de área de TIC y monitoreo de redes, así como las posibles estrategias de seguridad.																								
	3) Implementar medidas de seguridad: Servidor CentOS con norma ISO-IEC 27001:2013 para seguridad de Intranet de CFE Zona Cuautitlán	3.1 Evaluar herramientas y tecnologías para la implementación del servidor																								
		3.2.- Definir la configuración del servidor y de zabbix para su instalación																								
		3.3.- Implementar el servidor en la red local																								
		3.4 Realizar recomendaciones de uso de agentes para monitoreo de la red																								

Imagen 6 Calendario de actividades en base al objetivo específico durante la Residencia Profesional imagen 2. [Fuente Propia].

CAPÍTULO III

DESARROLLO

A continuación, se presentarán cada uno de los objetivos específicos a fin de describirlo y detallarlo a través de la realización de cada de una de sus actividades; cabe mencionar que en este punto resulta preciso explicar el desarrollo de cada una de estas actividades presentando los en conjunto con los resultados de esta, a fin de que exista orden y coherencia del proyecto.

TESCO

3.1 OBJETIVO ESPECÍFICO

1.- Evaluar el proceso actual de operación de monitoreo de las redes de intranet de Zona Cuautitlán

3.1.1 ACTIVIDAD A REALIZAR

1.1.- Realizar entrevista para conocer a la organización de forma general (contexto, políticas, infraestructura), la situación y si existen controles por parte del departamento de TIC de Zona Cuautitlán.

En este objetivo se pretende alcanzar con el desarrollo de las actividades el análisis de la situación en los controles de seguridad, la infraestructura, conocimientos y contexto de la organización por parte del departamento de TICs y la definición de conceptos pertenecientes a la empresa.

DESCRIPCIÓN DE LA ACTIVIDAD

Como ya se mencionó, el objetivo de realizar una entrevista apoyada de un cuestionario es conocer el contexto, políticas, infraestructura y la situación con respecto a la operatividad y seguridad del departamento de TIC de Zona Cuautitlán. Las siguientes preguntas fueron contestadas por el Ing. Gregorio Escobedo Obregón, jefe del departamento de TIC en CFE Zona Cuautitlán, con la intención de conocer acerca de la organización y específicamente en el departamento que el administra y la situación en la red de Cuautitlán Izcalli.

RESULTADO DE LA ACTIVIDAD

Entrevista para conocer el contexto de la organización CFE

1.- Hábleme a cerca de sus funciones como jefe del departamento de TICs.

Soy el jefe de departamento de Tecnologías de la Información en la zona Cuautitlán, y mi función es el de administrar las TICs, ofrecer soporte y aplicar buenas prácticas para mantener segura la información.

2.- ¿Qué es la seguridad de la información?

Lineamientos, políticas y prácticas que se establecen para mantener, resguardar los sistemas, informaciones inherentes a una organización.

3.- Mencione aspectos de la infraestructura de la red en la zona

El tráfico en la red es filtrado por MAC Address, la controladora de wifi está en oficinas divisionales, aquí en zona Cuautitlán solo se puede configurar las IP de los equipos o conectar los mismos a la red wifi, pero la administración del wifi no es posible realizarla nosotros

Los equipos de cómputo están registrados en un inventario, se concentran en un servidor OCS Inventory a nivel divisional. Solamente se puede dar de alta y baja, la administración no se lleva a cabo aquí, es a nivel divisional.

Para actualizar Windows, a nivel zona se tiene un servidor Wsus, ya que, al trabajar dentro de una intranet, no se tiene salida a los sistemas de Microsoft, solamente en horarios específicos y fuera de labores, esta administración y permisos para conectarse a Microsoft es a nivel nacional.

Los equipos de la zona pueden solo conectarse a dos tipos de redes; esta la red de TI que es la red administrativa o corporativa de CFE, y la red OT que es la red operativa. El departamento de TICs administra la red administrativa, la red OT es ajena al departamento de TICs de zona Cuautitlán.

La red que administro son dos enlaces de fibra óptica de 60 MB/S, desde oficinas divisionales hasta aquí a la zona Cuautitlán. Uno está contratado por CFE Telecom y el segundo es rentado por Telmex, este último es de respaldo.

La mayoría de los switches que administro son de capa 3, el direccionamiento IP para computadoras por medio de cable es estático, por red wifi es dinámico. Yo no controlo la red wifi, solo algunos segmentos de la misma red que están asignados a mí y son locales.

4.- ¿Cuentan con políticas de seguridad para las redes?

Si contamos

5.- ¿Dónde las puedo conseguir?

Pueden ser encontradas en la página normateca.cfemex.com, solo es accesible si se está conectado a la intranet.

6.- ¿Existen manuales y registros como guía para solucionar o anticipar las consecuencias de las amenazas?

Si, existe una guía de sanitización de equipos de cómputo, se encuentra en los archivos de CFE en la intranet en el SISAT (página web interna) y contiene políticas, acuerdos y procedimientos de CFE a nivel nacional.

7.- Me puede dar un ejemplo de cómo aplica las políticas en la red

Los equipos de cómputo deben estar registrados en el inventario de directorio activo, el antivirus debe estar actualizado e instalado y en el caso de la wifi, se tiene un filtrado por MAC address.

8.- ¿Qué amenazas existen podrían afectar la intranet?

No recibimos ataques informáticos en 13 años, y en cuanto a fenómenos naturales en 2017 cayó un rayo en la torre de Zumpango se cayeron los enlaces, la conexiones con los enlaces de la red, todos los servicios de cfe telecom.

9.- Mencione controles existentes para evitar las amenazas

Aplicación de antivirus corporativo y actualización mediante consola del antivirus (actualización centralizada), b) Filtrado MAC en redes inalámbricas, conexión inalámbrica mediante filtrado MAC, C) Actualización de sistemas operativos mediante servidor WSUS.

10.- ¿Cuántos incidentes se suscitan al año aproximadamente y que tan grave sería?

No se han suscitado ataques, debido a que recibimos reportes de posibles vulnerabilidades y estos se atienden a la brevedad con impacto alto si se presentase.

11.- ¿A tenido problemas con los usuarios?

En cuanto a mal uso de los equipos, siguiendo indicaciones o problemas de seguridad.

12.- ¿De qué marca y modelo son los dispositivos para la comunicación de la red?

Son switches capa 2 y capa 3, routers, access point, se usan marca cisco, telefonía.

13.- ¿Cuáles son sus proveedores de conexión a internet y de dispositivos de red?

Proveedor de servicio de internet es Telmex, los dispositivos de red son cisco y son proporcionados por la empresa.

14.- ¿Qué oportunidades existen y existieron, para mejorar la intranet de la empresa en la zona?

La obtención de servicios de red y tecnologías son consolidadas a nivel nacional, no elegimos los proveedores ni promociones. El avance tecnológico, no se puede controlar la compra de qué dispositivos o tecnologías utilizar.

15.- ¿Qué debilidades podría tener la red actualmente?

El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos.

16.- ¿Cuáles son las fortalezas de la intranet de la zona?

El jefe de departamento de TICs tiene certificación de cisco, lo cual tiene la capacidad y preparación para resolver problemas que se presenten

(Gregorio, 2023)

TESCO

3.1.2. ACTIVIDAD A REALIZAR

Realizar una entrevista sobre el área problemática en monitoreo de redes de la zona Cuautitlán

DESCRIPCIÓN DE LA ACTIVIDAD

De igual manera que el anterior cuestionario, este segundo, contiene preguntas más precisas sobre las posibles áreas de oportunidad a mejorar con respecto a esta evaluación. También estas preguntas fueron contestadas por Ing. Gregorio Escobedo Obregón, jefe del departamento de TIC en CFE Zona Cuautitlán, con la intención de conocer acerca de la situación en cuanto a monitoreo de redes en Cuautitlán Izcalli, si existen controles, conocimiento y expectativas.

RESULTADO DE LA ACTIVIDAD

Entrevista para conocer el área problemática

1.- La red que usted administra (TI) ¿Cuenta con algún control de monitoreo?

No. Solo es monitoreada la disponibilidad de los equipos a nivel divisional

2.- Mencione tres amenazas que comprometerían la seguridad de las redes y su nivel de impacto negativo en la empresa

a) No contar con inventario de direccionamiento IP con bajo impacto, b) no contar con seguridad en las redes inalámbricas con impacto alto c) contar con equipos sin antivirus o desactualizados con impacto alto

3.- ¿Qué tan probable es que existan anomalías en el ancho de banda y que impacto tiene el ancho de banda para la empresa?

Saturación y retraso en los trabajos del personal. Una vez al trimestre, a nivel de usuarios se puede perder atención a solicitudes, de saturarse se pierde la comunicación vía wifi, la información de entrada o salida será lenta. El impacto en la empresa es alto.

El enlace principal tiene 60 Mb para la intranet de manera asíncrona. Estos 60 Mb están destinados para los departamentos de administración, trabajo, operación, mantenimiento, comercial, medición conexiones y servicios, planeación y construcción, jurídico, TICs de CD Victoria en Zona Cuautitlán y para los CD Zumpango, las Américas, Coyotepec

4.- ¿Cómo soluciona este problema?

Solicitar un nuevo enlace, solicitar un incremento de ancho de banda, fuera de ello no tengo control, por ello necesito monitorio de ancho de banda en puerto para tratar de minimizar el daño y revisar los equipos

5.- ¿Qué procesos, programas o actividades suelen consumir muchos recursos en el ancho de banda?

Teams en video conferencias, one drive, ftps, , navegación en varias

6.- ¿Qué tan probable es que existan anomalías en la velocidad de conexión y que impacto tiene para la empresa?

100 megas mínimo en conexión full dúplex. Su impacto es alto, no es tan perjudicial como la sobre saturación en el ancho de banda, pero atrasa los procesos de operación. Igualmente, solo se presenta poca velocidad cuando el ancho de banda se satura.

7.- ¿Qué tan probable es que existan interrupciones de servicio a internet y que impacto tiene para la empresa?

Una vez cada tres años, sin embargo, para la operatividad no requiero internet, la operatividad con lleva, por ejemplo, facturación, reconexiones, cobro de energía o cobranza, por que todo es dentro de la intranet. Por lo que su impacto sería mediano, ya que la empresa puede realizar todas sus actividades sin necesidad de internet, pero algunos procesos se verían ralentizados como la comunicación con los clientes, comprar tareas vía correo electrónico o reuniones.

8.- Implementar un control de monitoreo de red localmente, ¿Sería beneficioso para la organización?

Si, sería de gran ayuda que se monitoree la disponibilidad de los equipos, monitoreo por ICMP, ancho de banda, protocolo SNMP.

9.- ¿Qué expectativas tendría de implementarse un control de monitoreo, relacionado a los protocolos ICMP y SNMP u otro aspecto?

Justamente conocer el ping y consumo de recursos o ancho de banda de los equipos asignados

10.- De implementarse una herramienta de software para el monitoreo de la red, ¿Qué

sistema operativo considera el adecuado?

Interesaría de preferencia en Linux

(Gregorio, 2023)



TESCO

3.1.3. ACTIVIDAD A REALIZAR

1.3 Realizar cuestionarios a usuarios de 4 diferentes departamentos sobre el departamento de TICs.

DESCRIPCIÓN DE LA ACTIVIDAD

A fin de conocer el punto de vista de los usuarios sobre los servicios del departamento de TIC's, se realizaron las siguientes preguntas fueron contestadas por los usuarios de los departamentos de administración, contabilidad, jurídico y mediciones, con la intención de conocer acerca de sus actividades en la empresa, buscando una relación entre sus labores y la experiencia dentro de la intranet.

RESULTADO DE LA ACTIVIDAD

Cuestionario usuarios

Departamento de Administración

1.- ¿Alguna vez sus labores se han visto interrumpidas por problemas con sus equipos de cómputo?

Rara vez

2.- ¿Cuáles han sido esos incidentes, que ocurrió, fue relacionado a una página web, correo electrónico o programa en especial?

Problema con la red, se perdió la conexión hacia internet, con la intranet no he tenido problemas

3.- ¿Con que frecuencia ocurrió?

Rara vez

4.- ¿Qué tan pronta es la resolución del problema?

Si, la resolución es rápida

5.- ¿Qué programas normalmente ocupas?

Sao, paquetería, correo electrónico,

6.- ¿Qué páginas normalmente utilizas?

Hermes, RIJ (por parte de cfe), campus CFE

7.- ¿Qué actividades normalmente realizas?

Hacer tutoriales, oficios

8.- ¿Sabes cómo funciona una intranet?

No realmente

9.- ¿Conoces si CFE tiene una intranet?

Si

Si la respuesta es sí:

10.- ¿Has tenido problema con la intranet?

No

11.- ¿Qué actividades realizas en la intranet?

Envío de documentos

12.- ¿Qué fortalezas o características positivas ves en el departamento de TICs?

La accesibilidad de el personal de tics y la atención hacia nosotros

13.- ¿Consideras que tengan debilidades el departamento de TICs?

Falta de personal personal

14.- ¿Existe algo que pueda perjudicar al departamento de TICs?

Temas personales externos que afecten emociones y concentración para realizar las actividades

15.- ¿Hay algo que recomendarías para el departamento? O ¿Alguna propuesta sobre algo que pudiesen mejorar?

No, solo que sea más eficiente, tiene que ver con personal o disponibilidad de tiempo

Departamento de Administración/ oficina de contabilidad

1.- ¿Alguna vez sus labores se han visto interrumpidas por problemas con sus equipos de cómputo?

Si, va muy lenta, se tuvo que formatear, y tardaron un día

2.- ¿Cuáles han sido esos incidentes, que ocurrió, fue relacionado a una página web, correo electrónico o programa en especial?

En ocasiones el computador va lenta, una vez me tuvieron que formatear la computadora

3.- ¿Con que frecuencia ocurrió?

Una vez al año

4.- ¿Qué tan pronta es la resolución del problema?

Tardan un poco, tardo un día

5.- ¿Qué programas normalmente ocupas?

SAP, SIAD

6.- ¿Qué páginas normalmente utilizas?

SISAO y páginas institucionales

7.- ¿Qué actividades normalmente realizas?

Capitalización de obras

8.- ¿Sabes cómo funciona una intranet?

No bien, son páginas dentro de cfe

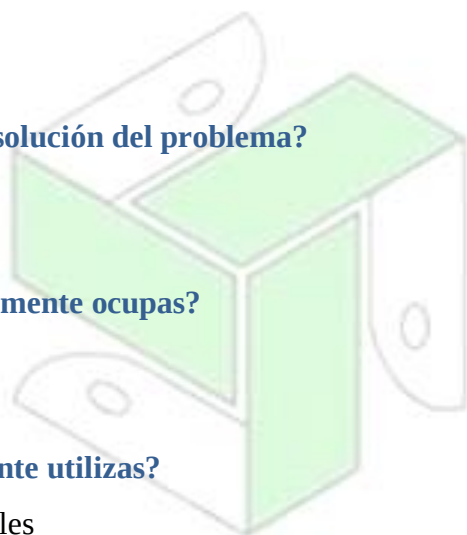
9.- ¿Conoces si CFE tiene una intranet?

si

Si la respuesta es sí:

10.- ¿Has tenido problema con la intranet?

A veces



TESCO

11.- ¿Qué actividades realizas en la intranet?

Capitalización de obras en SISAO, en la web normal no se puede abrir

12.- ¿Qué fortalezas o características positivas ves en el departamento de TICs?

Tienen actitud para hacer el trabajo

13.- ¿Consideras que tengan debilidades el departamento de TICs?

Si, demora en las actividades

14.- ¿Existe algo que pueda perjudicar al departamento de TICs?

No creo

15.- ¿Hay algo que recomendarías para el departamento? O ¿Alguna propuesta sobre algo que pudiesen mejorar?

Tienen mucha carga de trabajo, por lo mientras no podría proponer algo.

Departamento de Jurídico

1.- ¿Alguna vez sus labores se han visto interrumpidas por problemas con sus equipos de cómputo?

No ninguna vez

2.- ¿Cuáles han sido esos incidentes, que ocurrió, fue relacionado a una página web, correo electrónico o programa en especial?

Se desconImagen la impresora

3.- ¿Con que frecuencia ocurrió?

No recuerdo

4.- ¿Qué tan pronta es la resolución del problema?

Si rápidamente, si hay apoyo rapido

5.- ¿Qué programas normalmente ocupas?

Teams, office, sinot y sicos

6.- ¿Qué páginas normalmente utilizas?

Outlook

7.- ¿Qué actividades normalmente realizas?

Recuperación de energía

8.- ¿Sabes cómo funciona una intranet?

Más o menos

9.- ¿Conoces si CFE tiene una intranet?

Si

Si la respuesta es sí:

10.- ¿Has tenido problema con la intranet?

No

11.- ¿Qué actividades realizas en la intranet?

Cargar los cortes y sacar ordenes de cortes de energía eléctrica

12.- ¿Qué fortalezas o características positivas ves en el departamento de TICs?

Me han solucionado las cosas muy rápidas, y las pocas veces que he necesitado ayuda me resuelven rápidamente

13.- ¿Consideras que tengan debilidades el departamento de TICs?

No

15.- ¿Existe algo que pueda perjudicar al departamento de TICs?

Desconozco

16.- ¿Hay algo que recomendarías para el departamento? O ¿Alguna propuesta sobre algo que pudiesen mejorar?

No en realidad, estoy bastante cómodo y satisfecho con la atención y trabajo que dedican

Departamento de OSC Mediciones

1.- ¿Alguna vez sus labores se han visto interrumpidas por problemas con sus equipos de cómputo?

Por computo no, de internet algunas veces

2.- ¿Cuáles han sido esos incidentes, que ocurrió, fue relacionado a una página web, correo electrónico o programa en especial?

No solamente conexión, muy rara vez

3.- ¿Con que frecuencia ocurrió?

Rara vez

4.- ¿Qué tan pronta es la resolución del problema?

normal

5.- ¿Qué programas normalmente ocupas?

SICO, SIMET (propias de CFE)

6.- ¿Qué páginas normalmente utilizas?

SESESNAL, SICOS WEB (propias de CFE)

7.- ¿Qué actividades normalmente realizas?

Área de medidores y asignación de trabajos

8.- ¿Sabes cómo funciona una intranet?

No como tal no

9.- ¿Conoces si CFE tiene una intranet?

Si

Si la respuesta es sí:

9.- ¿Has tenido problema con la intranet?

Si, red wifi se desconecta de repente por no tener ethernet

10.- ¿Qué actividades realizas en la intranet?

Área de medidores y asignación de trabajos

11.- ¿Qué fortalezas o características positivas ves en el departamento de TICs?

El tiempo de respuesta y atención

12.- ¿Consideras que tengan debilidades el departamento de TICs?

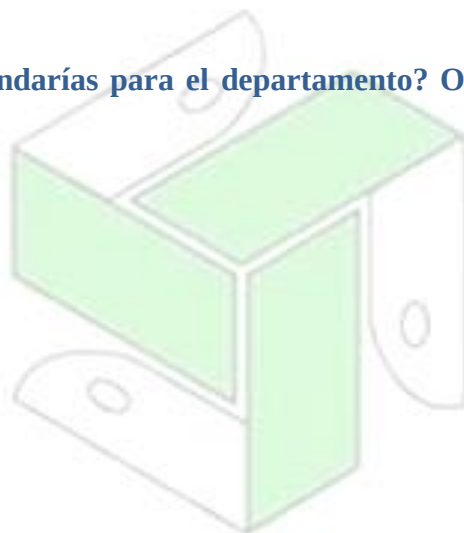
Algunas veces la capacidad de proceso, necesitan más personal

14.- ¿Existe algo que pueda perjudicar al departamento de TICs?

Vacaciones o incapacidades medicas

15.- ¿Hay algo que recomendarías para el departamento? O ¿Alguna propuesta sobre algo que pudiesen mejorar?

No por el momento



TESCO

3.2.OBJETIVO ESPECÍFICO

2.- Diagnosticar el área de TIC'S, enfocándose en el proceso actual de operación de monitoreo de las redes de intranet de Zona Cuautitlán.

3.2.1. ACTIVIDAD A REALIZAR

2.1.- Diagnosticar con un análisis de Fortaleza, Oportunidades, Amenazas y Debilidades del departamento de TIC de Zona.

DESCRIPCIÓN DE LA ACTIVIDAD

Cómo parte de entender el contexto del área de TICs, se han formado varios análisis que permite plasmar las Fortaleza, Oportunidades, Debilidades y Amenazas (FODA), que consentirá tener el contexto interno y externo, visualizando con claridad lo bueno y malo que existe en esta área. Este documento surge de la información recopilada al entrevistar a los usuarios sobre sus actividades y experiencias dentro de la red, software y herramientas, al igual que de la entrevista al jefe del departamento de TICs, sus políticas, lineamientos, contexto, infraestructura y monitoreo en la red; formulando así tres FODA's, el primero es resultado de la información obtenida del departamento de TICs, el segundo de la información obtenida de los usuarios y un tercer resulta de ambos FODA's previos.

RESULTADO DE LA ACTIVIDAD

Departamento de TICs de la zona Cuautitlán

Análisis: La siguiente tabla FODA está constituida por la información obtenida del personal de TIC's. Los elementos en ella (fortaleza, debilidades, oportunidades y amenazas) se destacan por enfocarse en las características propias de TIC's y su entorno, no considerando como tal el contacto directo con los usuarios.

Tabla 1 Análisis FODA por miembros del departamento de TIC's. [Fuente Propia].

FORTALEZAS	DEBILIDADES
Cuenta con controles de seguridad en la intranet como: -Contar con antivirus corporativo -Filtrado MAC de redes inalámbricas -Actualización de sistema operativo mediante servidor WSUS	El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos

Tabla 2 Análisis FODA por miembros del departamento de TIC's.(Continuación) [Fuente Propia].

FORTALEZAS	DEBILIDADES
Personal capacitado, con experiencia de trece años en el departamento, que puede hacerse cargo de la TIC y resolver problema que se presenten	Desconocimiento de usuarios sobre seguridad de la información y uso de los recursos de la red
Sus procesos están basados en sus políticas de seguridad a nivel nacional	Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad
Tienen inventario de equipos	La administración de la red wifi esta fuera del alcance de TICs. No es controlada por el departamento
Cuentan con un enlace de fibra óptica de respaldo de 60 MB	La red wifi esta fuera de nuestra administración
OPORTUNIDADES	AMENAZAS
No se puede controlar la decisión de compra de qué dispositivos o tecnologías utilizar.	Factores ambientales, cuales, como terremotos o tormentas eléctricas
Limitaciones de presupuesto	Ataques por parte de delincuentes informáticos
Documentación y registros de los procesos que se realizan en el departamento de TIC falta ser complementado	Interrupciones de energía eléctrica
	Avances tecnológicos que dejen desactualizados los equipos informáticos o procesos de la empresa

Análisis FODA obtenido de la información de usuarios

Del siguiente planteamiento se puede concluir que los usuarios tienen una percepción únicamente de la atención de TIC's hacia la resolución rápida o lenta de sus necesidades, lo cual da como resultado un FODA breve y sencillo, pero permite ver otro ángulo diferente al previamente realizado al departamento de TIC's. La explicación se puede explicar a que el personal de TIC's ve un entorno basado en sus herramientas, su capacidad y dificultades, mientras los usuarios visualizan la manera en que son tratados, el tiempo y eficacia de la resolución de sus problemas.

Tabla 3 Análisis FODA por usuarios de los departamentos dependientes de TIC's [Fuente Propia].

FORTALEZAS	DEBILIDADES
Rápida reacción del personal de TICs para resolver problemas	Demora en resolución de problemas
Buena actitud y atención hacia los usuarios	
El personal de TICs es gente muy capaz y amplios conocimientos	Gran carga de trabajo para el personal de TICs
	Poco personal de TICs

	Poca disponibilidad de tiempo, debido al poco personal de TICs
--	--

Tabla 4 *Análisis FODA por usuarios de los departamentos dependientes de TIC's (Continuación)*[Fuente Propia].

OPORTUNIDADES	AMENAZAS
Asignación de más personal al equipo de TIC	Temas personales externos que afecten emociones y concentración para realizar las actividades
	Vacaciones, al solo contar con dos elementos, el que tengan vacaciones hace más complicado la resolución de problemas

Análisis FODA RESULTANTE

Finalmente, se construye un FODA resultante de usuarios y departamento de TIC's. En base a cada fortaleza, debilidad, oportunidad y amenaza, se puede evaluar posteriores estrategias, trabajar y definir los riesgos más importantes, de estos mismos riesgos obtener valores, métricas y niveles de priorización.

Tabla 5 *Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.* [Fuente Propia].

FORTALEZAS	DEBILIDADES
Rápida reacción del personal de TICs para resolver problemas Descripción: Se resuelve a la brevedad posible las dificultades y problemas que se presentan en los equipos de los usuarios	El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos Descripción: El ancho de banda es compartido de manera asíncrona (quiere decir que no hay un límite impuesto de cuanto recurso de los 60 mb de banda ancha se puede consumir) a todos los departamentos administrados por el departamento de TICs, además de otros centros de distribución ubicados en Zumpango, Huehuetoca, y Coyotepec, por lo que, si un departamento o centro consume demasiado, dejara sin recurso a los departamentos y centros restantes
	Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad Descripción: No se cuenta con monitoreo de equipos de usuarios. Esto provoca incertidumbre de que

	equipo o equipos consumen más de ancho de banda y el por que
--	--

Tabla 6 *Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.*(Continuación 1) [Fuente Propia].

	Demora en resolución de algunos problemas Descripción: El personal de TIC es escaso. Demora en la resolución de problemas en algunas actividades
Buena atención hacia los usuarios Descripción: El personal de TICs se presenta con buena actitud, atención y amabilidad ante las peticiones de los clientes	Gran carga de trabajo para el personal de TICs Descripción: El departamento de TICs administra los sistemas informáticos, inventario de los equipos, da soporte técnico, se encarga de la instalación de software, asignación de equipos, entre otras actividades, todo esto a los diferentes departamentos a su cargo, incluso a otros centros de distribución.
Priorización de resolución a problemas Descripción: Se resuelven primero aquellos problemas que tienen un mayor impacto negativo en los procesos de la empresa o que pudiese afectar a un número mayor de usuarios	Poco personal de TICs Descripción: Solo se cuenta con el apoyo de dos elementos en el personal de TICs. El jefe de departamento para los asuntos administrativos y un operativo para resolución a usuarios internos a la empresa
Cuenta con controles de seguridad en la intranet como: -Contar con antivirus corporativo -Filtrado MAC de redes inalámbricas -Actualización de sistema operativo mediante servidor WSUS Descripción: Se implementan controles acordes a sus políticas, a no utilizar herramientas de fuentes externas, ya que tienen las mismas dentro de sus servidores	Poca disponibilidad de tiempo, debido al poco personal de TICs Descripción: Las actividades del personal de TICs deben hacerse dentro de jornada laborales. A pesar de que las actividades administrativas y algún percance fuera de horario laboral y tickets pendientes se da seguimiento por el jefe de departamento de TICs, no pueden realizarse en un periodo corto de tiempo debido al poco personal de TICs

--	--

Tabla 7 Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.(Continuación 2) [Fuente Propia].

Cuentan con un enlace de fibra óptica de respaldo de 60 MB Descripción: El ancho de banda de la red es de 60 MB, en caso de necesitar más capacidad o de saturarse el tráfico de datos en la red, se tiene un respaldo de 60 MB más.	
Tienen inventario de equipos Descripción: Hacen uso de una herramienta de software llamado OCS Inventory, para registrar equipos, así como sus características y usuarios asignados	
Sus procesos están basados en sus políticas de seguridad a nivel nacional Descripción: Dentro de la intranet, en la página del SISAT Se encuentran las políticas de seguridad para TICs, establecidas a nivel nacional	
Personal capacitado, con experiencia de trece años en el departamento, que puede hacerse cargo de la TIC y resolver problema que se presenten Descripción: El personal del departamento de TICs cuenta con trece años de experiencia en el área dentro de la empresa. El jefe de departamento cuenta con certificados y título universitario	
OPORTUNIDADES	AMENAZAS
No se puede controlar la decisión de compra de qué dispositivos o tecnologías utilizar Descripción:	Factores ambientales, cuales, como terremotos o tormentas eléctricas Descripción:

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

La autorización de compra y que se puede implementar como tecnología es dada por las autoridades normativas a nivel nacional	Ya ha sucedido en el pasado. Cuando ocurre un desastre natural puede llegar a destruir o inhabilitar los activos y servicios, interrumpiendo procesos de la empresa, pérdida de comunicación y pérdidas económicas.
--	---

Tabla 8 Análisis FODA resultante del análisis por parte de TIC's y por parte de los usuarios.(Continuación 3) [Fuente Propia].

OPORTUNIDADES	AMENAZAS
Limitaciones de presupuesto Descripción: Si un presupuesto no se limitase, podría usarse para obtener licencias de herramientas de software que contribuyan o faciliten los procesos de TICs, por ejemplo, de contarse con presupuesto, se podría implementar sistemas de monitoreo completos y beneficios que se ven integrados en su contratación	Ataques por parte de delincuentes informáticos Descripción: Un ataque por malware, denegación de servicio o de cualquier tipo llega a ser catastrófico para cualquier organización, implica la pérdida, corrupción y disponibilidad de la información, lo que desencadena una interrupción de los procesos y pérdidas económicas.
Documentación y registros de los procesos que se realizan en el departamento de TIC falta ser complementado Descripción: Falta complementar documentación del estado de los equipos. El generar este tipo de documentación con lleva un mejor conocimiento de los activos y donde usarlos	Interrupciones de energía eléctrica Descripción: Muchos equipos informáticos no cuentan con no break, o conectados a una planta de energía de respaldo. Si llegase a ver una pérdida de energía eléctrica esto ralentiza la productividad de los usuarios, además que, en el proceso, aquellos que no guarden su información la perderán y tendrán que comenzar a rehacer lo perdido
Umbral de desconocimiento de seguimiento de actividades de los usuarios Descripción: Las actividades de los usuarios a precisión, de forma individual, se desconoce a grandes rasgos. Se monitorean los switches que conectan a los dispositivos de la red, pero no a los mismos dispositivos individualmente.	Temas personales externos que afecten emociones, física y la concentración para realizar las actividades Descripción: Situaciones familiares, económicas, accidentes o percances de cualquier tipo, pueden incapacitar física o mentalmente al personal de Tics para realizar adecuadamente sus actividades Avances tecnológicos que dejen desactualizados los equipos informáticos o procesos de la empresa Descripción: La empresa compra equipos y dispositivos de cómputo y redes entre 5 a 10 años. Además de no otorgar presupuesto suficiente para implementar

	softwares que requieran de un plus por lo tanto una paga mensual. Ello deja las tecnologías de TICs desactualizadas.
--	--

Conclusión: Los FODA, síntesis de las diferentes entrevistas y cuestionarios realizados tanto a usuarios como personal de TIC's, han sido recopilados en uno mayor cuya finalidad es concebir un análisis de riesgos sobre el área problemática que resulte con mayor prioridad, hilado de ello generar estrategias y ejecutar la más adecuada a la empresa.



TESCO

3.2.2. ACTIVIDAD A REALIZAR

2.2.- Diagnosticar con un análisis de riesgos sobre la situación actual del área problemática a apoyar

DESCRIPCIÓN DE LA ACTIVIDAD

Para la realización de este diagnóstico, fue en base a las recomendaciones de acuerdo con la norma **Internacional Organization for Standardization (ISO,2017), ISO-IEC 27001:2013, página 11**, en ella se menciona que considerar para el análisis de riesgos, de los cuales tres puntos son usables de acuerdo con el análisis FODA de la actividad previa:

- a) Establecer criterios de riesgos de la seguridad de la información (criterios de apreciación {criterios para considerar un evento un riesgo} y aceptación)
- c) Identificar los riesgos (identificar los riesgos y sus dueños o causantes)
- d) Analizar los riesgos (valorar las posibles consecuencias de los riesgos, valorar de forma realista la probabilidad de ocurrencia de los riesgos, determinar los niveles de riesgo)

Nota: Para saber más diríjase al anexo A.1 ISO-IEC 27001:2013 Análisis de riesgos.

RESULTADO DE LA ACTIVIDAD

Establecer criterios de riesgos de la seguridad de la información

Métricas

Criterios para considerar un evento un riesgo

En el documento interno P-Procedimiento Identificación de aspectos e impactos ambientales, peligros y evaluación de riesgos y oportunidades de seguridad y salud en el trabajo, dentro de la intranet de CFE sección 4.2.3.2.1 Evaluación de Riesgos Simple, página 21 establece preguntas para la evaluación de riesgos. Por lo que se tiene conocimiento de riesgos, controles y prevenciones, entre otros, sin embargo, no aplicado de la misma manera, controlado y estructurado a la seguridad informática.

Para generar los criterios de aceptación de riesgos, identificación de riesgos, riesgos y sus dueños se han formulado preguntas adaptadas al contexto de seguridad de la información y TIC's como guía, todo ello conforme a lo antes mencionado en la norma ISO-IEC 27001:2013, las encuestas y entrevistas realizadas en las actividades y el documento interno.

Preguntas para los criterios de aceptación de riesgos

¿Con que frecuencia e impacto puede presentarse un evento?

¿Cómo puede afectar a la empresa?

¿Qué puedo hacer al respecto?

¿Qué niveles de aceptación habría?

Tabla 9 Indicadores de riesgo y prioridad de atención. [Fuente Propia].

RIESGO (Indicador)	CRITERIO DE CONSIDERACIÓN (apreciación)	DESCRIPCIÓN	PRIORIDAD DE ATENCIÓN
Crítico Intolerable	Ocurre con relativa frecuencia (frecuente, moderadamente o casi nunca) y de presentarse impacta de forma catastrófica a la empresa Puede ocasionar: -Pérdida de activos -Pérdida de vidas -Pérdida económica mayor a \$100,000 -Pérdida y corrupción de información	No es posible aceptar este tipo de riesgo, siempre debe contar la organización con un plan de recuperación, respaldo, vías alternas, y debe atenderse a la brevedad posible como prioridad. Basado en las circunstancias, las labores se verán interrumpidas.	URGENTE
Alto Intolerable	Ocurre con relativa frecuencia (frecuente, moderadamente o casi nunca) y de presentarse tiene un impacto alto negativo en la empresa Puede ocasionar: -Pérdida de activos -Pérdida económica menor a \$100,000 – Mayores a \$10,000 -Pérdida y corrupción de información	No es posible aceptar este tipo de riesgo, siempre debe contar la organización con un plan de recuperación, respaldo, vías alternas, y debe atenderse a la brevedad posible	ALTA

Tabla 10 Indicadores de riesgo y prioridad de atención. (Continuación) [Fuente Propia].

Medio Moderable	Ocurre con relativa frecuencia (frecuente, moderadamente o casi nunca) y de presentarse, tiene un impacto moderado en la empresa Puede ocasionar: -Atraso en los procesos -ralentización de obtención de información -Pérdidas económicas mayores a \$10,000 y menores a \$100,000	Una situación de peligro moderado puede crecer y escalar a un riesgo mayor, por lo que no se recomienda aceptarlo, por lo que contar con vías alternas y de tratamiento previene el crecimiento del riesgo. Si se acepta, se debe estar consciente de que los procesos se ralentizaran	MODERADA
Bajo Aceptable	Ocurre con relativa frecuencia (frecuente, moderadamente o casi nunca) y de presentarse, tiene un impacto bajo en la empresa Puede ocasionar: -ralentización en los procesos -Pérdidas económicas menores a \$10,000	No representa un peligro alto, sin embargo, algunos riesgos pueden ir escalando a niveles de altos si se ignoran. Puede ser aceptable, pero se recomienda atender el problema y asegurar que no desencadene otros riesgos.	BAJA

Identificación de los riesgos

La siguiente tabla indica el valor para considerar la frecuencia de ocurrencia de un riesgo como bajo, medio o alto.

Tabla 11 Indicador de ocurrencia. [Fuente Propia].

Ocurrencia	
Bajo	(0-1 vez al año)
Medio	(2-3 veces al año)
Alto	(4 o más veces al año)

La siguiente tabla indica el valor para considerar el impacto que puede tener un riesgo como bajo, medio, alto o crítico.

Tabla 12 Indicador de impacto. [Fuente Propia].

Impacto			
Bajo	Medio	Alto	Crítico

Del resultado entre la relación Impacto-Ocurrencia se obtiene la valoración de riesgo.

El riesgo y daño de un evento aumenta conforme más impacto tiene en la empresa, así, si un evento fuese de poca probabilidad y un alto impacto, tendera a ser clasificado como un riesgo

alto. Si es un impacto es bajo, tiende a ser de riesgo bajo, a menos que este se repita constantemente.

Tabla 13 Valoración de riesgo de acuerdo a impacto y ocurrencia. [Fuente Propia].

Valoración de Riesgo respecto Impacto / Ocurrencia			
Ocurrencia Impacto	Bajo (0-1 vez al año)	Medio (2-3 veces al año)	Alto (4 o más veces al año)
Bajo	Bajo aceptable	Bajo aceptable	Medio Moderable
Medio	Bajo aceptable	Medio Moderable	Alto Intolerable
Alto	Alto Intolerable	Alto Intolerable	Alto Intolerable
Critico	Critico Intolerable	Critico Intolerable	Critico Intolerable

La prioridad de atención a un riesgo se verá aumentada conforme más impacto tiene en la empresa y frecuencia tiene en la empresa. Los riesgos críticos ocasionan daños catastróficos en la empresa, por lo que, aunque su probabilidad sea baja, deben atenderse urgentemente. El orden de prioridad va de la más importante (número 1) a la menos importante (número 12).

Tabla 14 Matriz de prioridad de atención de acuerdo a impacto y ocurrencia. [Fuente Propia].

Tabla Matriz Prioridad de Atención respecto Impacto / Ocurrencia			
Ocurrencia Impacto	Bajo (0-1 vez al año)	Medio (2-3 veces al año)	Alto (4 o más veces al año)
Bajo	Baja (12)	Baja (11)	Moderada (8)
Medio	Baja (10)	Moderada (9)	Alta (6)
Alto	Alta (7)	Alta (5)	Alta (4)
Critico	Urgente (3)	Urgente (2)	Urgente (1)

El siguiente recuadro muestra la información de la matriz anterior desde la perspectiva de tabla:

Tabla 15 Tabla de prioridad de atención de acuerdo a impacto y ocurrencia. [Fuente Propia].

Prioridad de Atención respecto Impacto / Ocurrencia		
Impacto	Probabilidad	Prioridad
Bajo	Bajo	Baja (12)
Medio	Bajo	Baja (10)
Alto	Bajo	Alta (7)
Critico	Bajo	Urgente (3)
Bajo	Medio	Baja (11)
Medio	Medio	Moderada (9)
Alto	Medio	Alta (5)
Critico	Medio	Urgente (2)

Tabla 16 Indicadores de riesgo y prioridad de atención.(Continuación) [Fuente Propia].

Bajo	Alto	Moderada (8)
Medio	Alto	Alta (6)
Alto	Alto	Alta (4)
Critico	Alto	Urgente (1)

Para el llenado de la siguiente métrica Tabla de Valoración de riesgo se hizo un cuestionamiento a diez usuarios divididos entre los departamentos de contabilidad, administración, jurídico y servicios generales, y a dos usuarios del área de TIC's, los cuales se les pregunto sobre el impacto que significa la forma en que los eventos de vulnerabilidad y amenazas afecta a la empresa, y la probabilidad que significa la ocurrencia del suceso ya comentadas en el FODA en la actividad **2.1.- Diagnosticar con un análisis de Fortaleza, Oportunidades, Amenazas y Debilidades del departamento de TIC de Zona.**

Tabla 17 Tabla de valoración de riesgo por el personal de TIC's. [Fuente Propia].

Valoración de Riesgo									
Riesgo	Valor Criterios	Probabilidad			Valor Criterios	Impacto			
		Bajo	Medio	Alto		Bajo	Medio	Alto	Critico
Vulnerabilidad 1: El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	2 usuarios	0	Impacto	0	2 usuarios	0	0
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es medio, da igual a un riesgo Medio Moderable, con una prioridad Moderada (9) para atenderse							
Vulnerabilidad 2: Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	0	2 usuarios	Impacto	0	0	2 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es alto y el impacto es alto, da igual a un riesgo Alto Intolerable, con una prioridad Alta (4) para atenderse							

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 18 Tabla de valoración de riesgo por el personal de TIC's.(Continuación 1) [Fuente Propia].

Vulnerabilidad 3: Demora en resolución de algunos problemas	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	2 usuarios	0	Impacto	2 usuarios	0	0	0
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es bajo, da igual a un riesgo Bajo aceptable, con prioridad Baja (10) para atenderse							
Vulnerabilidad 4: Gran carga de trabajo para el personal de TICs	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	0	2 usuarios	Impacto	0	0	2 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es alto y el impacto es alto, da igual a un riesgo Alto Intolerable, con una prioridad Alta (4) para atenderse							
Vulnerabilidad 5: Poco personal de TICs	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	0	2 usuarios	Impacto	0	0	2 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es alto y el impacto es alto, da igual a un riesgo Alto Intolerable, con una prioridad Alta (4) para atenderse							
Vulnerabilidad 6: Poca disponibilidad de tiempo, debido al poco personal de TICs	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	0	2 usuarios	Impacto	0	0	2 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es alto y el impacto es alto, da igual a un riesgo Alto Intolerable, con una prioridad Alta (4) para atenderse							
Amenaza 1: Factores ambientales, cuales, como terremotos o tormentas eléctricas	¿Qué probabilidad considera que este evento ocurra en la empresa?	2 usuarios	0	0	Impacto	0	2 usuarios	0	0
	Valoración de Riesgo	La probabilidad de ocurrencia es bajo y el impacto es medio, da igual a un riesgo Bajo aceptable, con prioridad Baja (10) para atenderse							

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 19 Tabla de valoración de riesgo por el personal de TIC's.(Continuación 2) [Fuente Propia].

Amenaza 2: Ataques por parte de delincuentes informáticos	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	2 usuarios	0	Impacto	0	0	0	2 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es Media y el impacto es crítico, da igual a un riesgo Critico Intolerable, con prioridad Urgente (2) atenderse							
Amenaza 3: Interrupciones de energía eléctrica	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	2 usuarios	0	Impacto	0	2 usuarios	0	0
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es medio, da igual a un riesgo Medio Moderable, con prioridad Moderada (9) para atenderse							
Amenaza 4: Temas personales que afecten emociones, física y la concentración para realizar las actividades	¿Qué probabilidad considera que este evento ocurra en la empresa?	2 usuarios	0	0	Impacto	2 usuarios	0	0	0
	Valoración de Riesgo	La probabilidad de ocurrencia es baja y el impacto es bajo, da igual a un riesgo, Bajo Aceptable, con prioridad Baja (12) atenderse							
Amenaza 5: Avances tecnológicos que dejen desactualizados los equipos informáticos o procesos de la empresa	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	2 usuarios	0	Impacto	0	2 usuarios	0	0
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es medio, da igual a un riesgo Medio Moderable, con prioridad Moderada (9) para atenderse							

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 20 Tabla de valoración de riesgo por los usuarios de departamentos. [Fuente Propia]

Valoración de Riesgo									
Riesgo	Valor	Probabilidad			Valor	Impacto			
	Criterios	Bajo	Medio	Alto	Criterios	Bajo	Medio	Alto	Critico
Vulnerabilidad 3: Demora en resolución de algunos problemas	¿Qué probabilidad considera que este evento ocurra en la empresa?	3 usuarios	5 usuarios	2 usuarios	Impacto	0	7 usuarios	3 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es medio, da igual a un riesgo Medio Moderable, con una prioridad Moderada (9) para atenderse							
Vulnerabilidad 4: Gran carga de trabajo para el personal de TICs	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	4 usuarios	6 usuarios	Impacto	0	2 usuarios	8 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es alto y el impacto es alto, da igual a un riesgo Alto Intolerable, con una prioridad Alta (4) para atenderse							
Vulnerabilidad 5: Poco personal de TICs	¿Qué probabilidad considera que este evento ocurra en la empresa?	0	4 usuarios	6 usuarios	Impacto	0	0	8 usuarios	2 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es alto y el impacto es alto, da igual a un riesgo Alto Intolerable, con prioridad de Alta (4) para atenderse							
Vulnerabilidad 6: Poca disponibilidad de tiempo, debido al poco personal de TICs	¿Qué probabilidad considera que este evento ocurra en la empresa?	3 usuarios	5 usuarios	2 usuarios	Impacto	0	6 usuarios	3 usuarios	1 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es medio, da igual a un riesgo Medio Moderable, con prioridad Moderada (9) para atenderse							

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 21 Tabla de valoración de riesgo por los usuarios de departamentos. (Continuación), [Fuente Propia].

Amenaza 1: Factores ambientales, cuales, como terremotos o tormentas eléctricas	¿Qué probabilidad considera que este evento ocurra en la empresa?	8 usuarios	2 usuarios	0	Impacto	3 usuarios	4 usuarios	0	3 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es bajo y el impacto es medio, da igual a un riesgo Bajo aceptable, con prioridad Baja (10) para atenderse							
Amenaza 2: Ataques por parte de delincuentes informáticos	¿Qué probabilidad considera que este evento ocurra en la empresa?	8 usuarios	1 usuarios	1 usuarios	Impacto	1 usuarios	0	0	9 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es bajo y el impacto es crítico, da igual a un riesgo Critico Intolerable, con prioridad Urgente (3) atenderse							
Amenaza 3: Interrupciones de energía eléctrica	¿Qué probabilidad considera que este evento ocurra en la empresa?	3 usuarios	5 usuarios	2 usuarios	Impacto	0	0	9 usuarios	1 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es alto, da igual a un riesgo Alto Intolerable, con prioridad Alta (5) atenderse							
Amenaza 4: Temas personales externos que afecten emociones, física y la concentración para realizar las actividades	¿Qué probabilidad considera que este evento ocurra en la empresa?	2 usuarios	5 usuarios	3 usuarios	Impacto	0	1 usuarios	5 usuarios	4 usuarios
	Valoración de Riesgo	La probabilidad de ocurrencia es medio y el impacto es alto, da igual a un riesgo, Alto Intolerable, con prioridad Alta (5) atenderse							
Amenaza 5: Avances tecnológicos que dejen desactualizados los equipos informáticos o procesos de la empresa	¿Qué probabilidad considera que este evento ocurra en la empresa?	6 usuarios	1 usuarios	3 usuarios	Impacto	0	8 usuarios	2 usuarios	0
	Valoración de Riesgo	La probabilidad de ocurrencia es bajo y el impacto es medio, da igual a un riesgo Bajo aceptable, con prioridad Baja (10) atenderse							

Conclusión

Los riesgos y sus dueños (factor causante) y porque se materializan, son obtenidas en las tablas superiores en previos análisis de cuestionarios y FODA's, resultando a continuación una síntesis del análisis de riesgos. La siguiente tabla contiene esta información:

Tabla 22 Tabla síntesis del análisis de riesgos. [Fuente Propia]

Riesgo	Causantes	Eventos que lo materializan	Probabilidad de ocurrencia por año	Impacto	Valoración del Riesgo
Debilidad 1: El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos	Factor Humano	Una gran cantidad de usuarios y/o de uso excesivo de los recursos en la red ocasiona ralentización de transmisión de datos, pérdida de información, por ende, afecta a los procesos	Medio (2 – 3 veces al año)	Medio	Medio
Debilidad 2: Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad	Factor Humano	El uso de la herramienta incorrecta, gratuita o limitada de software de monitoreo y la gran cantidad de equipos informáticos dificulta el monitoreo individual y de comportamiento de los usuarios en la red	Alto (4 o más veces al año)	Alto	Alto
Debilidad 3: Demora en resolución de algunos problemas	Factor Humano	Poco personal asignado y la gran demanda de tareas que con lleva las TIC dificulta el proceso de resolución de problemas	Medio (2 – 3 veces al año)	Medio	Medio Moderable
Debilidad 4: Gran carga de trabajo para el personal de TICs	Factor Humano	Poco personal asignado y la gran demanda de tareas que con lleva las TIC producen una carga de labores a realizar	Alto Alto (4 o más veces al año)	Alto	Alto Intolerable
Debilidad 5: Poco personal de TICs	Factor Humano	Se cuenta con dos usuarios para atender las actividades del departamento de TICs.	Alto Alto (4 o más veces al año)	Alto	Alto Intolerable

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Tabla 23 Tabla síntesis del análisis de riesgos. (Continuación), [Fuente Propia].

Debilidad 6: Poca disponibilidad de tiempo, debido al poco personal de TICs	Factor Humano	Se priorizan las actividades a resolver por parte del departamento de TIC's	Medio (2 – 3 veces al año)	Medio	Medio Moderable
Amenaza 1: Factores ambientales, cuales, como terremotos o tormentas eléctricas	Naturaleza	Causas naturales. Afecta en la eficiencia de las actividades de los usuarios, por igual a los procesos	Bajo (0 – 1 vez al año)	Medio	Bajo Aceptable
Amenaza 2: Ataques por parte de delincuentes informáticos	Factor Humano	Brechas de seguridad explotadas por obsolescencia tecnológica, desconocimiento de los usuarios sobre seguridad informática o usuarios con intención.	Bajo (0 – 1 vez al año)	Crítico	Crítico Intolerable
Amenaza 3: Interrupciones de energía eléctrica	Factor Humano	Producidas por personas pertenecientes o ajenas a la empresa, sin o con intenciones. Los fenómenos naturales como fuertes lluvias, vientos o temblores pueden interrumpir el servicio eléctrico.	Medio (2 – 3 veces al año)	Alto	Alto Intolerable
	Naturaleza				
Amenaza 4: Temas personales externos que afecten emociones, física y la concentración para realizar las actividades	Factor Humano	Situaciones personales complicadas o accidentes pueden desestabilizar física, mental o emocionalmente a una persona.	Medio (2 – 3 veces al año)	Alto	Alto Intolerable
	Naturaleza				
Amenaza 5: Avances tecnológicos que dejen desactualizados los equipos informáticos o procesos de la empresa	Factor Humano	El constante crecimiento de la tecnología, y así mismo adquiriendo estas por parte de algunas empresas tanto de servicios, proveedores o socias, pueden dejar obsoletos algunos equipos informáticos o software con el que se opere.	Bajo (0 – 1 vez al año)	Medio	Bajo Aceptable

3.2.3. ACTIVIDAD A REALIZAR

2.3.- Genera informe que integre amenazas y vulnerabilidades de área de TIC y monitoreo de redes, así como las posibles estrategias de seguridad.

DESCRIPCIÓN DE LA ACTIVIDAD

En base al análisis de riesgos, el análisis FODA y los cuestionarios realizados, las vulnerabilidades y amenazas más evidentes estuvieron relacionadas con la cantidad de labores de TIC's para poco personal, interrupciones eléctricas y posibles ataques informáticos que podrían derivarse del poco conocimiento que los usuarios tienen acerca de la seguridad de la información y el mejor uso de los recursos de los equipos, programas y datos que son utilizados en sus labores diarias. Además de que no se cuenta con un monitoreo preciso de cada uno de los equipos de los usuarios, que en el caso de suceder un pico en el uso de ancho de banda que ocasionaría el impedimento de usar ese recurso en otras actividades u otros usuarios, no se ubicaría con exactitud qué equipo está consumiendo demasiado o presenta anomalías. Es así en el reporte presentado a continuación se retoma la información hallada sobre vulnerabilidades y amenazas en el área de TIC's, añadiendo las estrategias y recomendaciones que pueden llevarse a cabo para solucionar o prevenir estos eventos no deseados de acuerdo con la norma 27001:2013 y otras normas similares.

RESULTADOS DE LA ACTIVIDAD

La siguiente tabla representa la relación entre vulnerabilidades que puedan ser potenciadas por una amenaza y afecte a la seguridad de la información.

Tabla 24 Relación Vulnerabilidad/Amenaza. [Fuente Propia]

Vulnerabilidad		Amenaza
El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos	Puede ser explotada por	Ataques por parte de delincuentes informáticos
Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad	Puede ser explotada por	Ataques por parte de delincuentes informáticos
Demora en resolución de algunos problemas	Puede ser explotada por	Ataques por parte de delincuentes informáticos
		Interrupciones de energía eléctrica
		Temas personales externos que afecten emociones, física y la concentración para realizar las actividades

Tabla 25 Relación Vulnerabilidad/Amenaza, (Continuación). [Fuente Propia]

Gran carga de trabajo para el personal de TICs	Puede ser explotada por	Ataques por parte de delincuentes informáticos
		Interrupciones de energía eléctrica
		Factores ambientales, cuales, como terremotos o tormentas eléctricas
Poco personal de TICs	Puede ser explotada por	Temas personales externos que afecten emociones, física y la concentración para realizar las actividades
Poca disponibilidad de tiempo, debido al poco personal de TICs	Puede ser explotada por	

Estrategias y recomendaciones

Las siguientes tablas contienen las recomendaciones basadas en normas de seguridad de la información. Estas recomendaciones explican en que nos ayudan las normas adaptadas a una vulnerabilidad y lo que podría aplicarse, además de una estrategia, la cual toma las recomendaciones y las normas para dar solución a la vulnerabilidad o amenaza con mayor detalle, inclusive proponiendo métricas.

Las tablas se muestran ordenadas en orden de prioridad de menor a mayor.

Tablas de Vulnerabilidades

Tabla No.1 Contexto

Las vulnerabilidades nombradas como:

Debilidad 3; Demora en resolución de algunos problemas

Debilidad 4; Gran carga de trabajo para el personal de TICs

Debilidad 5; Poco personal de TICs

Debilidad 6; Poca disponibilidad de tiempo, debido al poco personal de TICs

están íntimamente relacionadas. Deben asignarse recomendaciones y diseñar estrategias para analizarse y mitigarse/evitarse en conjunto.

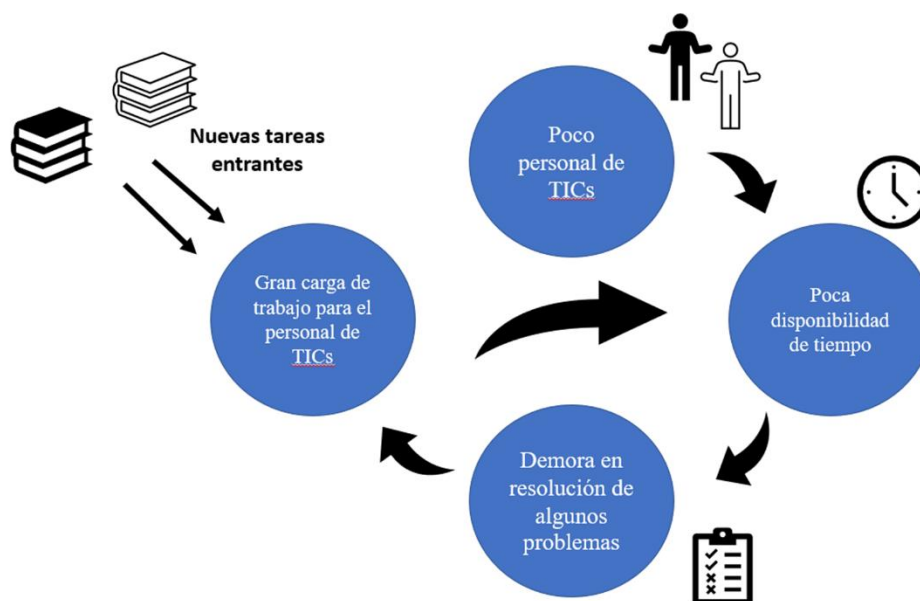


Imagen 7 Relación Poco personal en TIC's con otras vulnerabilidades. [Fuente Propia]

El departamento de TICs solo cuenta con dos usuarios para realizar las labores, no solo en la zona Cuautitlán, además dan soporte en otras zonas que requieran soluciones de TIC, esto se presenta mayormente cuando se otorgan periodos vacacionales, por ausencias u otras razones que no permitan estar presente a los elementos de TICs de distintas sedes.

Contar con dos usuarios en TICs propicia a que exista poca disponibilidad del tiempo para resolver incidentes y actividades diarias, ocasionando demoras y una gran carga de trabajo, sumando las posibles nuevas tareas o labores entrantes, manteniendo de esta manera un ciclo de vulnerabilidades.

A continuación, se presentan las recomendaciones y estrategias que pueden aplicarse en base al marco de trabajo COBIT 4.0 e ISO-IEC 27001:2013 para dar posibles soluciones que agilicen los procesos y mayores resultados de satisfacción de resolución de problemas que atiende el departamento de TICs.

Tabla 26 Recomendaciones para vulnerabilidades relacionadas a la poca eficiencia en TIC's. [Fuente Propia]

Vulnerabilidad	Prioridad
Poco personal de TICs	Alta (4)
Poca disponibilidad de tiempo, debido al poco personal de TICs	Moderada (9)
Demora en resolución de algunos problemas	Moderada (9)
Gran carga de trabajo para el personal de TICs	Alta (4)
Recomendación	
COBIT 4.0	
<u>El marco de trabajo COBIT 4.0, control DS3 Administrar el desempeño y la capacidad, página 111 a 114</u>, se enfoca en evaluar en periodos establecidos el desempeño y capacidad de los recursos de TI, esto debería incluir tanto activos en dispositivos, consumibles, materiales y personal. Con ayuda de este marco de trabajo, se busca el evaluar el desempeño y capacidad de TICs y en que se puede mejorar y planificar para que la disponibilidad de tiempo del personal de TICs sea acorde a las necesidades de la empresa y sus usuarios, además que se tenga previsto la necesidad de más personal para TICs. Medidas preventivas: Se debe prevenir las contingencias, necesidades o actividades futuras, con ello, la designación y disponibilidad de los recursos adecuadamente. *El encargado de TICs así como sus supervisores y/o superiores, deben asignar las actividades de cada miembro de TICs, un periodo de tiempo para cada actividad y también periodos de evaluación de desempeño. *El encargado de TICs así como sus supervisores y/o superiores, deben autorizar los recursos, incluyendo los humanos, para aumentar la efectividad de las labores. *Formular un plan de mejora y evaluación continua, que sea medible y considerando parámetros como lo son el tiempo de actividad de los usuarios de TICs, tickets de incidentes resueltos y no resueltos, herramientas y procesos que permitan conocer la situación actual y futura. Se recomienda usar un modelo de medición de madurez. Todo lo anterior debe apegarse a las políticas de seguridad que rigen a las TICs. Medidas Correctivas: *Se recomienda monitorear regularmente la situación actual para conocer la carga de trabajo, el desempeño, la disponibilidad del servicio y capacidad con los recursos humanos y materiales actuales. Con esta información reunida, posteriormente generar acciones correctivas y de planificación. *A través de reportes de la situación, reúnanse el jefe de departamento de TICs con las autoridades competentes e involucradas en la gestión de las TICs para la toma de decisiones en la mejora del servicio que ofrece TICs.	

Tabla 27 Recomendaciones para vulnerabilidades relacionadas a la poca eficiencia en TIC's, (Continuación), [Fuente Propia].

*Aplica las medidas preventivas mencionadas en la parte superior antes de comenzar Medidas Correctivas. Nota: Para saber más diríjase al anexo B.1 COBIT 4.0 DS3 Administrar el desempeño y la capacidad				
ISO – IEC 27001:2013				
Obtenido de la norma Organization for Standardization (ISO,2017), ISO-IEC 27001:2013 Norma Española, página 29, Anexo A, el control recomendado es el siguiente: Nota: Para saber más diríjase al anexo A.2 ISO-IEC 27001:2013 Anexo A.16				
Anexo	Proceso	Actividad	Control	Justificación
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras	A.16.1.1 Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	Este control se aplica a la importancia que debe darse a planear y dejar en claro el rol de casa miembro de TICs, con la intención de que las responsabilidades y procesos no sean transmitidos de un miembro a otros o retrase el tiempo y calidad de resultados

Estrategia

Tanto la norma ISO-IEC 27001:2013 como el marco COBIT 4.0 mencionan la importancia de establecer las responsabilidades y procedimientos que deben realizarse para ejecutar rápida y efectivamente los incidentes dentro de la empresa. Del mismo marco COBIT se puede obtener las siguientes actividades e indicadores clave a desempeñar adaptados a la empresa CFE zona Cuautitlán para evaluar las responsabilidades, la capacidad, prevenir eventos futuros y el mejor uso de los recursos, el cual, para tratar esta vulnerabilidad, es el tiempo de disponibilidad.

Las autoridades y personal involucrados deberán planear la evaluación y periodos de estas. Si la vulnerabilidad se encuentra en la poca disponibilidad de tiempo, deberán medir la cantidad con la que disponen y cuantos incidentes se han resuelto en esa situación. Finalmente analizar el desempeño y capacidad con los recursos actuales, incluyendo la disponibilidad, prever incidentes futuros y elaborar un plan, asignando responsabilidades y recursos.

La siguiente tabla propuesta se diseñó en base a la gráfica RACI, métricas y metas de la página 113 de COBIT 4.0:

Nota: Para saber más diríjase al anexo B.2 COBIT 4.0 Gráfica RACI

Tabla 28 Matriz relación entre miembros, indicadores y actividades a realizar para tratar las vulnerabilidades relacionadas a la poca eficiencia en TIC's. [Fuente Propia]

		Personal al que corresponde				
		Superintendencia	Jefe de departamento de TICs	Personal de TICs		
Actividades	Establecer un plan de evaluación y periodicidad de esta	X	X		Frecuencia de evaluación y pronósticos	Indicadores
	Evaluar la disponibilidad de tiempo y la cantidad de incidentes resueltos		X	X	Horarios laborales	
					Como se usa el tiempo de labores	
					Cantidad de tickets e incidentes resueltos	
	Revisar el desempeño y capacidad actual de los recursos de TICs		X		Cantidad de recursos	
					Medir Eficacia y eficiencia	
	Pronosticar incidentes futuros, plan de contingencia y la asignación de recursos para mitigarlos	X	X		Analizar problemas o eventos futuros	
					Desarrollar un plan	
					Autorizar los recursos necesarios	

La estrategia se puede resumir en los siguientes incisos:

A) Definir por parte del jefe de TICs y autoridades involucradas en su gestión, las responsabilidades, recursos humanos y procesos que ejecutarán los usuarios de TICs para un mejor servicio

B) Desarrollo de métricas de evaluación y registro de tickets en la solución de incidentes para medir el desempeño y capacidad de recursos, disponibilidad y futuros eventos

Al finalizar la evaluación debe asignarse los recursos necesarios para permitir mayor disponibilidad de tiempo para el personal de TICs, sea una mejor estructuración de sus procesos y responsabilidades como la asignación de mayor personal.

Para medir la madurez de los procesos y actividades, puede hacerse uso de un modelo de Madurez, como se muestra a continuación:

No-existente: Por parte del departamento o autoridades involucradas no hay entendimiento de los riesgos, vulnerabilidades y amenazas en la TI y como impactaría al negocio o empresa.

Inicial/Ad Hoc: La respuesta ante incidentes es de forma reactiva y sin previa planeación o preparación.

No se presta atención a la calidad de servicio de TI, en cambio los usuarios pueden llegar a buscar soluciones alternas, esto dice sobre la responsabilidad de los involucrados como autoridades o miembros del departamento de TI, siendo su responsabilidad y autoridad de forma informal y limitada.

Repetible pero intuitivo: Existe compromiso y sistemas de recolección de datos como inventarios, además de procedimientos, sin embargo, son incompletos tanto en estructura, no muy eficientes y los servicios se realizan sin satisfacción completa.

Proceso definido: Las responsabilidades y procedimientos son definidas y llevadas a cabo. Se recibe capacitación, los miembros de TI tienen iniciativa, siguen las políticas y estándares. Se tiene una estructura sólida.

Administrado y medible: Las responsabilidades y estándares se cumplen y son aplicados a las TI. En los reportes se recopila y analiza información que sirva para una mejora continua, tanto a los procesos, la continuidad del servicio y capacitación obligatoria del personal. Se aplican buenas prácticas.

Optimizado: Se consideran estrategias y buenas prácticas incluso externas relacionadas a la industria. Los planes de mejora continua se apegan a las necesidades y dirección de la empresa. Las pruebas y evaluaciones en el departamento se hacen en conjunto a los demás departamentos de la empresa, en todo aspecto y son garantizados por los proveedores y distribuidores. Los reportes se utilizan para mejorar constantemente los resultados y servicios obtenidos y ofrecidos.

La siguiente tabla del modelo de madurez está basada en lo descrito por COBIT 4.0 en la página 118 del marco de trabajo:

Nota: Para saber más diríjase al anexo B.3 COBIT 4.0 Modelo de Madurez

Modelo de Madurez de los Procesos y Actividades para TICs					
				NIVEL 5 Optimizado	
			NIVEL 4 Administrado y medible	Proceso #	
		NIVEL 3 Proceso definido	Proceso #	Proceso #	
	NIVEL 2 Repetible pero intuitivo	Proceso #	Proceso #	Proceso #	
	NIVEL 1 Inicial	Proceso #	Proceso #	Proceso #	
NIVEL 0 No existe	Proceso #	Proceso #	Proceso #		
Proceso 1	Proceso #	Proceso #			
Proceso 2	Proceso #				
Proceso 3					

Imagen 8 Propuesta de modelo de madures de los procesos. [Fuente Propia]

Tabla No.2 Contexto

La vulnerabilidad **El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos** pudiese ser atacada solamente al existir una sobrecarga de tráfico en la red, quiere decir, si los usuarios hacen mal uso de los recursos en la red o existiese un ataque informático, la red se saturaría y colapsaría.

Los usuarios pertenecientes a la intranet y no exclusivos del departamento de TICs, no tienen conocimientos o cuentan con poco sobre seguridad de la información. Esta situación deriva en hacer mal uso de los recursos de red, que, si bien cuenta con filtros de seguridad y restricciones por firewall para restringir el acceso a páginas dañinas o poco productivas, esto no impide que descarguen o transmitan información en grandes cantidades, innecesaria o contaminada.

La educación y concientización de los usuarios debe impartirse de acuerdo con las necesidades de su jerarquía y labores dentro de la empresa.

Las siguientes recomendaciones y estrategias ayudaran a la toma de decisiones para prevenir la saturación del ancho de banda a través de la concientización de usuarios y cómo actuar si se presenta.

Nota: Para una mayor protección en la red, considere las recomendaciones y estrategias de la **tabla No.3 Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad.**

TESCO

Tabla 29 Recomendaciones para vulnerabilidad relacionada al ancho de banda. [Fuente Propia]

Vulnerabilidad	Prioridad
El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos	Moderada (9)
Recomendación	
COBIT 4.0	
<u>El marco de trabajo COBIT 4.0, control DS7 Educar y entrenar a los usuarios, página 127 a 130</u>, se recomienda diseñar e impartir un programa de entrenamiento de usuarios, para el uso adecuado de los recursos de la red y de seguridad de la información. Cada programa será elaborado de acuerdo con las políticas de seguridad de la empresa, las necesidades y nivel de acceso de los usuarios. Posterior a ello, se debe medir el nivel de efectividad. Gracias al monitoreo de las actividades de los usuarios, se puede conocer más información al respecto. Medidas preventivas *Las autoridades o individuos involucrados en las TICs deben reunirse para la toma de decisiones de un plan de capacitación para los usuarios. *Conocer las necesidades y límites de los usuarios según el departamento y nivel de acceso que tengan. Con ello realizar un plan de capacitación *Aplicar el plan de capacitación a los usuarios y con ayuda de métricas, evaluar los conocimientos y efectividad del buen uso de los recursos de la red en los usuarios. *Mejorar las capacitaciones y evaluar en periodos regulares de tiempo la efectividad. Medidas correctivas *Las autoridades o individuos involucrados en las TICs deben reunirse para la toma de decisiones de la situación actual, carencias y de incidentes suscitados. *Desarrollar un plan de capacitación para los usuarios. Se debe conocer las necesidades y límites de los usuarios según el departamento y nivel de acceso que tengan. A la par, de presentarse un evento que afecte a la empresa relacionado a esta vulnerabilidad, debe asignarse recursos y personal de TICs para solucionar la situación. *Aplicar el plan de capacitación a los usuarios y con ayuda de métricas, evaluar los conocimientos y efectividad del buen uso de los recursos de la red en los usuarios. *Mejorar las capacitaciones y evaluar en periodos regulares de tiempo la efectividad. Nota: Para saber más diríjase al anexo B.4 COBIT 4.0 DS7 Educar y entrenar a los usuarios	
ISO – IEC 27001:2013	
Obtenido de la norma Organization for Standardization (ISO,2017), ISO-IEC 27001:2013 Norma Española, página 26 y 29, Anexo A, el control recomendado es el siguiente: Nota: Para saber más diríjase al anexo A.3 ISO-IEC 27001:2013 Anexo A.13, A.16	

Tabla 30 Recomendaciones para vulnerabilidad relacionada al ancho de banda. (Continuación) [Fuente Propia]

Anexo	Proceso	Actividad	Control	Justificación
A.13 Seguridad de las comunicaciones	A.13.1 Gestión de la seguridad de las redes	A.13.1.1 Notificación de los eventos de seguridad de la información	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	El monitoreo de redes es un control de seguridad aplicado en la empresa, sin embargo, a nivel usuario, quiere decir, individualmente a cada usuario dentro de un departamento con equipo asignado a él, no está siendo monitoreado.
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras	A.16.1.2 Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible	Los usuarios deben advertir ante cualquier anomalía a al departamento de TICs para verificar y dar solución en caso de un incidente

Estrategia

Si bien la empresa cuenta con políticas de seguridad y controles para asegurar que toda información sea compartida únicamente en la intranet y restringir el acceso total o parcial a internet, el ancho de banda, lo que permite el envío y recibo de datos entre los diferentes departamentos, usuarios y procesos puede verse comprometida por el desconocimiento de los usuarios sobre seguridad, ello puede propiciar un mal uso de los recursos o una brecha de seguridad para que un agente externo ataque.

Tabla 31 Estrategias resultantes de la relación vulnerabilidad/amenaza. [Fuente Propia]

	El consumo de ancho de banda del enlace principal, solo se tiene 60 megabytes asíncronos
Amenaza Ataques por parte de delincuentes informáticos	A) Educar a los usuarios sobre los riesgos y buen uso de los recursos informáticos de la intranet de CFE Zona Cuautitlán. B) Evaluar la efectividad a través de análisis y métricas sobre el conocimiento y rendimiento de la red

Tanto la norma ISO-IEC 27001:2013 como el marco COBIT 4.0 mencionan la importancia de establecer las responsabilidades y procedimientos que deben realizarse para una continuidad efectiva, de servicios, evaluación e implementación. Del mismo marco COBIT se obtiene las siguientes actividades e indicadores clave a desempeñar adaptados a la empresa CFE zona Cuautitlán para evaluar la capacitación y resultados dados a usuarios para su educación.

Las autoridades y personal involucrados deberán planear la evaluación y periodos de estas.

La siguiente tabla propuesta se diseñó en base a la gráfica RACI, métricas y metas de la página 129 de COBIT 4.0:

Nota: Para saber más diríjase al anexo B.5 COBIT 4.0 Gráfica RACI.



Tabla 32 Matriz relación entre miembros, indicadores y actividades a realizar para tratar las vulnerabilidades relacionadas a la educación y concientización de los usuarios. [Fuente Propia]

		Personal al que corresponde				
		Superintendencia	Jefe de departamento de TICs	Personal de TICs		
Actividades	Identificar las necesidades y límites de usuarios para su capacitación	X			Nivel de acceso a la información	Indicadores
					Métodos y herramientas apropiados de capacitación	
	Construir un programa de capacitación	X	X		Nivel de acceso a la información	
					% de usuarios	
					Métodos y herramientas apropiados de capacitación	
	Implementar el programa de capacitación e impartirlo	X	X	X	% de usuarios	
					Recursos destinados	
					Temas tratados	
	Evaluar e identificar los métodos y herramientas que han sido útiles y mejorarlas o expandirlas	X	X		% de satisfacción de los usuarios	
					% de incidentes	
					% de usuarios capacitados	

Para la educación y entrenamiento de los usuarios de diferentes departamentos incluyendo los de TICs, se debiera:

- 1) Considerar las estrategias. Políticas, valores corporativos y requerimientos actuales y

futuros en dirección conjunta a la empresa

- 2) Conocer las habilidades, perfiles, límites, nivel de acceso a la información de los usuarios
- 3) Designar recursos e instructores para cada diferente grupo de usuarios
- 4) Construir la capacitación, elegir como se impartirá, por cuales canales de información, lugares, tiempos y la implementación de herramientas de software que complementen a al aprendizaje
- 5) Evaluar la capacitación y su efectividad con respecto a los resultados por parte de los usuarios como lo es su conocimiento, satisfacción de los cursos, efectividad y el costo/recursos que ha designado la empresa.

Tabla No. 3 Contexto

Los dispositivos se pueden monitorear a través de los switches, pero solamente aquella información que es recolectada a través de los puertos donde se conectan. El protocolo ICMP permite el conocer si aquellos equipos están disponibles y transmitiendo o recibiendo datos.

Los switches en la empresa son monitoreados con ayuda de la herramienta PRTG PAESSLER usando el protocolo SNMP, sin embargo, este software está limitado a 100 sensores para la versión gratuita. No se usa una versión de pago debido a que no esté autorizado presupuesto.

Se requiere una herramienta de monitoreo que permita sin límite el monitorear equipos conectados a una red, esto permite recolectar más características gratuitamente de un solo dispositivo.

Conocer más información y características ayuda a tener un mejor control y mayor alcance para prevenir ataques informáticos y un inadecuado uso de los ordenadores o switches.

Se proponen las siguientes recomendaciones y estrategias:

Tabla 33 Recomendaciones para vulnerabilidad relacionada al monitoreo en la red. [Fuente Propia]

Vulnerabilidad				Prioridad
Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad				Alta (4)
Recomendación				
Obtenidos de la norma Organization for Standardization (ISO,2017) , ISO-IEC 27001:2013, página 24,25 y 29, Anexo A, los controles recomendados que se adaptan a la situación y posterior mejora en la organización son los siguientes:				
Nota: Para saber más diríjase al anexo A.4 ISO-IEC 27001:2013 Anexo A.12, A.16				
Anexo	Proceso	Actividad	Control	Justificación
A.12 Seguridad de las operaciones	A.12.1 Procedimientos y responsabilidades operacionales	A.12.1.1 Documentación de procedimientos operacionales	Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten	Al implementar la estrategia de seguridad, debe documentarse el funcionamiento y procedimiento para que el personal a cargo conozca como utilizarlo
A.12 Seguridad de las operaciones	A.12.4 Registros y supervisión	A.12.4.1 Registro de eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información	El monitoreo de red ofrece registrar, revisar, notificar las actividades de los usuarios en la red y posterior el actual para proteger la información en caso de un evento peligroso
A.16 Gestión de incidentes de seguridad de la información	A.16.1 Gestión de incidentes de seguridad de la información y mejoras (todas)	A.16.1.2 Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	

Estrategias

Una de las oportunidades que afecta indirectamente a las vulnerabilidades y amenazas es el no contar con la aprobación de un presupuesto para la contratación de software de licencia, cuya

finalidad es que permita el uso de mejores herramientas para el control y monitoreo de los equipos. Además de tratarse de un requerimiento por parte de la empresa, el uso de software o cualquier otra tecnología sin costo alguno.

Considerando los principales requerimientos de la empresa, exponiendo su enfoque a los eventos críticos que puedan suscitarse por amenazas externa por delincuentes informáticos, por vulnerabilidades que puedan ocasionar los usuarios y las recomendaciones antes mencionadas, se genera la siguiente estrategia:

Tabla 34 Estrategias resultantes de la relación vulnerabilidad/amenaza para el monitoreo de red. [Fuente Propia]

	Debilidad Complicaciones en el monitoreo de equipos, solo se puede monitorear la disponibilidad
Amenaza Ataques por parte de delincuentes informáticos	A) Instalar y configurar un servidor y sus controles haciendo uso de software para el monitoreo del ping y protocolo SNMP en los equipos informáticos de la intranet de manera local en Zona Cuautitlán. B) Documentar y generar formatos para los registros de los puertos, estatus y a que equipos y usuarios están asignados para el departamento de TIC

Descripción estratégica

- A) Instalar y configurar un servidor y sus controles haciendo uso de software para el monitoreo del ping y protocolo SNMP en los equipos informáticos de la intranet de manera local en Zona Cuautitlán.**

El monitoreo debe realizarse con ayuda de software que permita obtener información tanto en datos como gráficamente para conocer los dos principales requerimientos de la empresa, el ping y el ancho de banda. Este tipo de software debe obtener la información sin necesidad de instalar agentes o programas extra a los equipos informáticos, solamente haciendo uso del servidor.

Opciones de software sugeridas

Las siguientes opciones no están ordenadas en ningún tipo de priorización, preferencia o eficacia/eficiencia de mayor a menor escala.

- 1) The Wireshark Network Analyzer – Sistema Operativo Windows
- 2) Zabbix – Sistema Operativo CentOS
- 3) Comparación PRTG

Cualquiera de estas herramientas de software debe instalarse en su sistema operativo correspondiente, a su vez, este sistema operativo se instalará en un dispositivo específicamente para su función como servidor de monitoreo, por lo que usarlo para otras actividades laborales no está permitido.

Para evaluar estas herramientas se propone la siguiente métrica haciendo uso de los controles recomendados en la norma ISO-IEC 27001:2013:

Tabla 35 Métrica de evaluación para herramienta de software. [Fuente Propia]

Control	Criterio	¿Cuenta con el criterio?			
		No cuenta (0)	Poco (1)	Regular (2)	Totalmente (3)
A.12.1.1 Documentación de procedimientos operacionales	Existe documentación				
	Cuenta con soporte técnico				
A.12.4.1 Registro de eventos	Genera reportes				
	La información se registra y almacena				
A.16.1.2 Notificación de los eventos de seguridad de la información	Cuenta con trigger de acciones ante eventos				
	Advierte de eventos o anomalías				
A.18.1.3 Protección de los registros de la organización	La herramienta / software es segura				
	Cuenta con respaldo				
Total:					

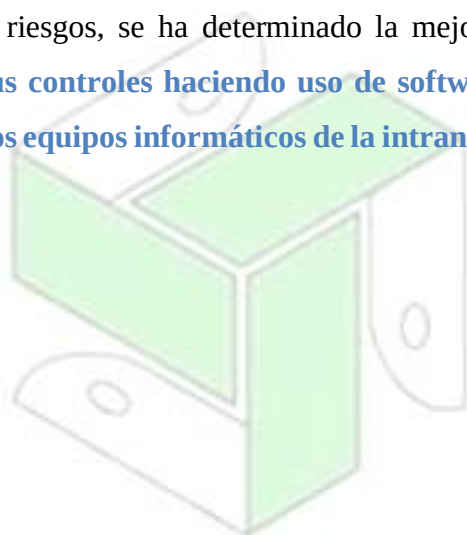
B) Documentar y generar formatos para los registros de los puertos, estatus y a que equipos y usuarios están asignados para el departamento de TIC

Complementario al monitoreo de equipos, se recomienda generar documentación y registro de que puertos están siendo utilizados, que equipos y usuarios han sido asignados.

La documentación para registro de la empresa puede ser realizado con herramientas que la misma entidad ya cuenta, como lo sería Excel, Word e inventario de equipos, además de comandos para conocer el estado de los puertos en los switches CISCO.

Conclusión

La necesidad principal expuesta por la empresa y retomando sus requerimientos, se determina se debe trabajar en un proyecto que permita monitorear los recursos de los usuarios, siendo un proyecto escalable y que se requiere como primeros dos objetivos el monitoreo de ping por ICM y SNMP. Evaluando las necesidades, requerimientos de la empresa, vulnerabilidad de poco monitoreo de los usuarios en la red y la amenaza que puede atacar esta vulnerabilidad encontrada en el análisis de riesgos, se ha determinado la mejor estrategia es “**Instalar y configurar un servidor y sus controles haciendo uso de software para el monitoreo del ping y protocolo SNMP en los equipos informáticos de la intranet de manera local en Zona Cuautitlán.**”



TESCO



CAPÍTULO IV RESULTADOS

En este último capítulo se presentan las estrategias de seguridad que se han permitido dejar funcionando en la empresa, así como una serie de recomendaciones para el ámbito de seguridad informática.

4.1. OBJETIVO ESPECÍFICO

3.- Implementar un Servidor CentOS con norma ISO-IEC 27001:2013 para seguridad de Intranet de CFE Zona Cuautitlán

4.1.1. ACTIVIDAD A REALIZAR

3.1.- Evaluar herramientas y tecnologías para la implementación del servidor

DESCRIPCIÓN DE LA ACTIVIDAD

De acuerdo a la estrategia A) **Instalar y configurar un servidor y sus controles haciendo uso de software para el monitoreo del ping y protocolo SNMP en los equipos informáticos de la intranet de manera local en Zona Cuautitlán**, mencionada en la actividad 2.3.- **Genera informe que integre amenazas y vulnerabilidades de área de TIC y monitoreo de redes, así como las posibles estrategias de seguridad**, y los controles propuestos en la métrica Tabla 21 Métrica de evaluación para herramienta de software, se evaluará las opciones de software recomendadas para el monitoreo de la intranet de CFE para la seguridad de la información. Finalmente comparar las herramientas y seleccionar la adecuada.

RESULTADO DE LA ACTIVIDAD

Herramientas de Software

The Wireshark Network Analyzer

Es un analizador gratuito de protocolos y paquetes de red. Analiza el contenido de los paquetes de información que son enviados en la red, además de capturar tráfico de otros medios de red como Ethernet, Wireless LAN, Bluetooth, USB.

WireShark no manipula ni envía datos a los dispositivos ni a la red.

Cuenta con las siguientes características:

Tabla 36 Ventajas/desventajas de wireshark. [Fuente Propia]

Ventajas/Beneficios	Desventajas
Inspección de miles de protocolos de red	No advierte cuando sucede alguna anomalía
Análisis de equipos encendidos y apagados	No toma acciones o igual a no contar con triggers
Multiplataforma	La interfaz gráfica tiene un grado medio de dificultad para ser operada
Utiliza como visualización GUI en buscadores web o vía TTY-mode	
Variedad de filtros para mostrar información	
La información puede ser leída desde diferentes protocolos como Ethernet, IEEE 802.11, Bluetooth, USB, Frame Relay, etc.	
Lectura y escritura de diferentes formatos para los archivos	

Requerimientos

- 1) “The Universal C Runtime; KB2999226” o el “KB3118401”,
- 2) procesador de 64-bit AMD64/x86-64 o 32-bit x86
- 3) 500 MB mínimo de RAM y Almacenamiento
- 4) Tarjeta de red

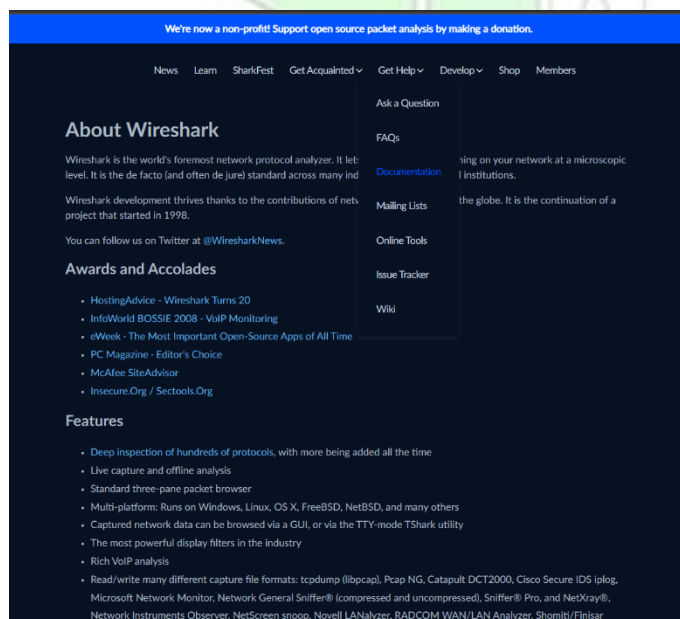


Imagen 9 Página principal de WireShark. [Fuente wireshark.org/about.html]

WireShark se puede descargar para Windows, macOS u obtener el código fuente:



Imagen 10 Descargas para WireShark. [Fuente wireshark.org/download.html]

La documentación de wireshark no se encuentra en grandes cantidades, debido a que es un software fácil de instalar y manejar, con gran uso, pero sin funciones de controlar ordenadores, o conocer aspectos indirectamente implicados en el monitoreo de red, pero los cuales son importantes o triggers avanzados.

Parte de su documentación está grabada en videos tutoriales oficiales de los desarrolladores de esta herramienta.



Imagen 11 Videos en la documentación de WireShark. [Fuente wireshark.org/docs/]

(WireShark, s.f.), (WireShark, s.f.)

Tabla 37 Métrica de evaluación para WireShark. [Fuente Propia]

Control	Criterio	¿Cuenta con el criterio?			
		No cuenta (0)	Poco (1)	Regular (2)	Totalmente (3)
A.12.1.1 Documentación de procedimientos operacionales	Existe documentación		X		
	Cuenta con soporte técnico			X	
A.12.4.1 Registro de eventos	Genera reportes		X		
	La información se registra y almacena			X	
A.16.1.2 Notificación de los eventos de seguridad de la información	Cuenta con trigger de acciones ante eventos	X			
	Advierte de eventos o anomalías	X			
A.18.1.3 Protección de los registros de la organización	La herramienta / software es segura			X	
	Cuenta con respaldo	X			
Total:		8 PUNTOS			

WireShark es una herramienta de gran uso para capturar el tráfico en la red, sin embargo, no es apto para servidor, no se puede usar como tal, ni contiene funciones que permitan administrar de manera SNMP u de otra forma la red. Al no tener este plus y no ser usado en entornos de Linux, no podría considerarse como la primera opción a usar en la empresa.

Zabbix

Es un software gratuito de código abierto para monitorear variedad de parámetros de las redes, estado e integridad de los servidores, máquinas virtuales, base de datos, servicios, aplicaciones, sitios web, entre otros.

Zabbix usa notificaciones vía e-mail para alertar sobre algún cambio o anomalía, ofrece reportes y estadísticas sobre los parámetros de lo que se esté monitoreando.

Algunas características de Zabbix obtenidas de su manual son las siguientes:

Tabla 38 Resumen características de Zabbix. [Fuente Propia]

Característica	Descripción
Recolección de datos	1) Comprobación de disponibilidad y rendimiento 2) Soporte para SNMP IPMI, JMX, VMware 3) Trabaja con servidores, proxy y agentes 4) Recolección y comprobaciones de datos personalizada
Configuración de alerta	1) El envío de alertas o notificaciones se pueden personalizar el tipo de medio y destinatario 2) Acciones automáticas incluye comandos remotos
Graficas en tiempo real	1) Los elementos monitoreados se grafican inmediatamente usando la funcionalidad gráfica incorporada
Monitoreo Web	1) Sigue la ruta de clics en un sitio web y el tiempo de respuesta
Amplias opciones de visualización	1) Personalización de gráficas, combinando parámetros o ítems en una sola vista 2) Mapa de red 3) Reportes 4) Vista de recursos monitoreados
Almacenamiento de datos	1) Datos guardados en una base de datos 2) Historial con Imagenble 3) Procedimientos de limpieza integrado
Plantillas	1) Comprobación de grupos 2) Plantillas pueden heredar de otras plantillas
Descubrimiento de redes	1) Descubrimiento de dispositivos de red automáticamente 2) Auto registraci3n de agentes 3) Descubrimiento de archivos de sistema
Interfaz Web	1) Accesible desde un navegador
Permisos de sistema	1) Autenticaci3n segura de usuarios 2) Algunos usuarios pueden ser limitados a ciertas vistas

El flujo de datos

Primeramente, debe crearse un host (dispositivo de red que se desea monitorear, cuenta con una IP o DNS) para crear un item(datos que se desean recibir desde un host) que recolecte datos, con el item se puede crear un trigger o alerta, posteriormente se crea una acción.

Entonces por ejemplo si se desea recibir una alerta de que la carga (número de procesos) de una CPU es muy alta en el servidor “X”, primero, debes crear una entrada de host para el servidor “X”, después un item para monitorear la CPU, entonces un trigger se activara al detectar una carga alta, la acción seria enviar un email de notificación o alerta.

Zabbix realiza procesos de forma automática, como lo menciona en su página oficial, trabaja en monitoreo y supresión de algunas anomalías que puedan presentarse en la red con ayuda de agentes y disparadores (triggers):

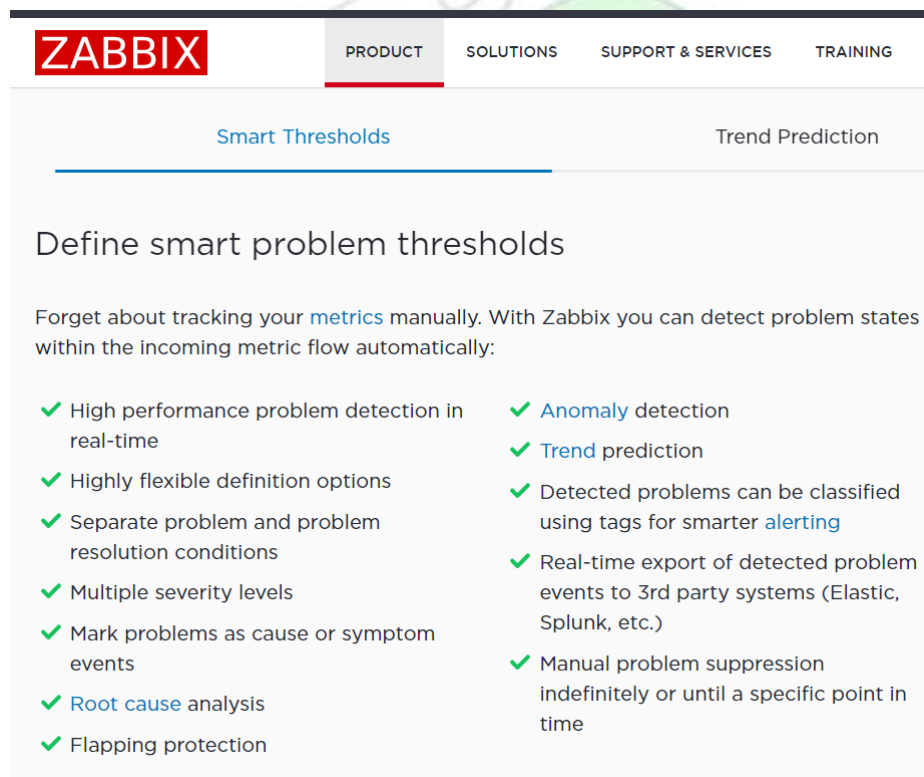


Imagen 12 Página web Zabbix definir limites en problemas.[Fuente zabbix.com/features]

Trabaja con variadas vistas de gráficas, mapa de red, inventarios y paneles para mostrar la información recolectada.

Zabbix cuenta con una gran documentación que explica como instalar zabbix en diferentes medios, sistemas operativos. Explica brevemente cómo funciona cada elemento de su servidor y agentes. Cuenta con una gran comunidad y la información es amplia, tanto oficial

como extraoficial.

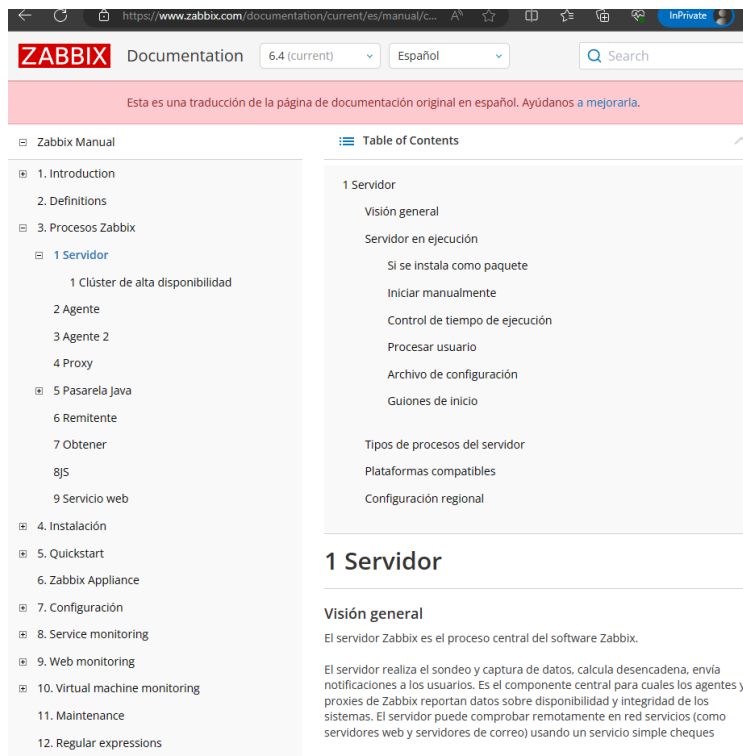


Imagen 13 Manual de zabbix sección servidor. [Fuente [zabbix.com/documentation/current/en/manual/concepts/server](https://www.zabbix.com/documentation/current/en/manual/concepts/server)]

Zabbix presenta una completa información y manuales al respecto, tanto para las diferentes versiones que se han liberado como los pre-requisitos de software, sistemas operativos donde se instalara, métodos de descarga e instalación, servidores locales, formas de instalar los softwares complementarios como MySQL, Postgre SQL, entre otros gestores y base de datos, sus mismos elementos de zabbix como agentes, servidor y proxy, entre otros.

Descarga e instalación de Zabbix

Zabbix
Paquetes

Imágenes
de nube
Images

Imágenes
Docker de
Zabbix

Zabbix
Appliance

Códigos
Fuentes de
Zabbix

Agentes
Zabbix

1

Elige tu plataforma

VERSIÓN ZABBIX	DISTRIBUCIÓN DE SO	VERSIÓN DEL SISTEMA OPERATIVO	ZABBIX COMPONENT	BASE DE DATOS	SERVIDOR WEB
6.4	Alma Linux	9	Server, Frontend, Agent	MySQL	Apache
6.0 LTS	CentOS	8	Proxy	PostgreSQL	Nginx
5.0 LTS	Debian		Agent		

Imagen 14 Selección descarga e instalación de zabbix. [Fuente zabbix.com/download]

Descarga e instala agentes Zabbix precompilados

For Agent DEBs and RPMs please visit [Zabbix packages](#)

☐ Show legacy downloads

DISTRIBUCIÓN DE SO	VERSIÓN DEL SISTEMA OPERATIVO	HARDWARE	VERSIÓN ZABBIX	ENCRIPCIÓN	EMBALAJE
Windows	Any	amd64	6.4	OpenSSL	MSI
Linux		i386	6.2	No encryption	Archive
macOS			6.0 LTS		
AIX			6.0		
FreeBSD			5.4		
OpenBSD			5.2		
Solaris			5.0 LTS		

Imagen 15 Selección descarga e instalación de zabbix imagen 2. [Fuente zabbix.com/download]

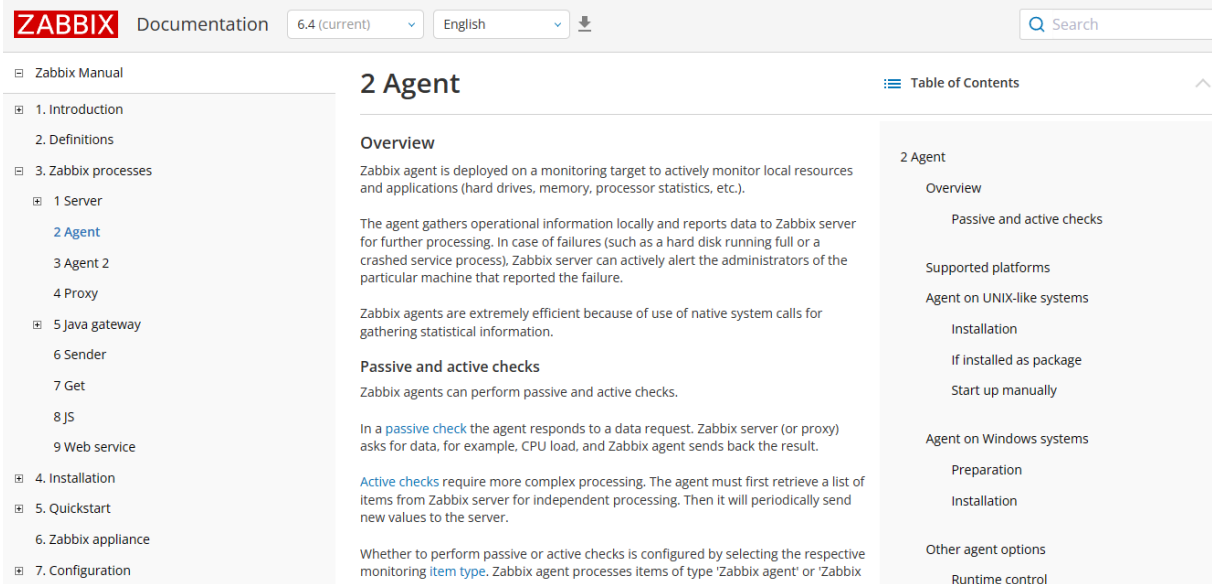


Imagen 16 Manual de zabbix sección Agente. [Fuente zabbix.com/documentation/current/en/manual/concepts/agent]

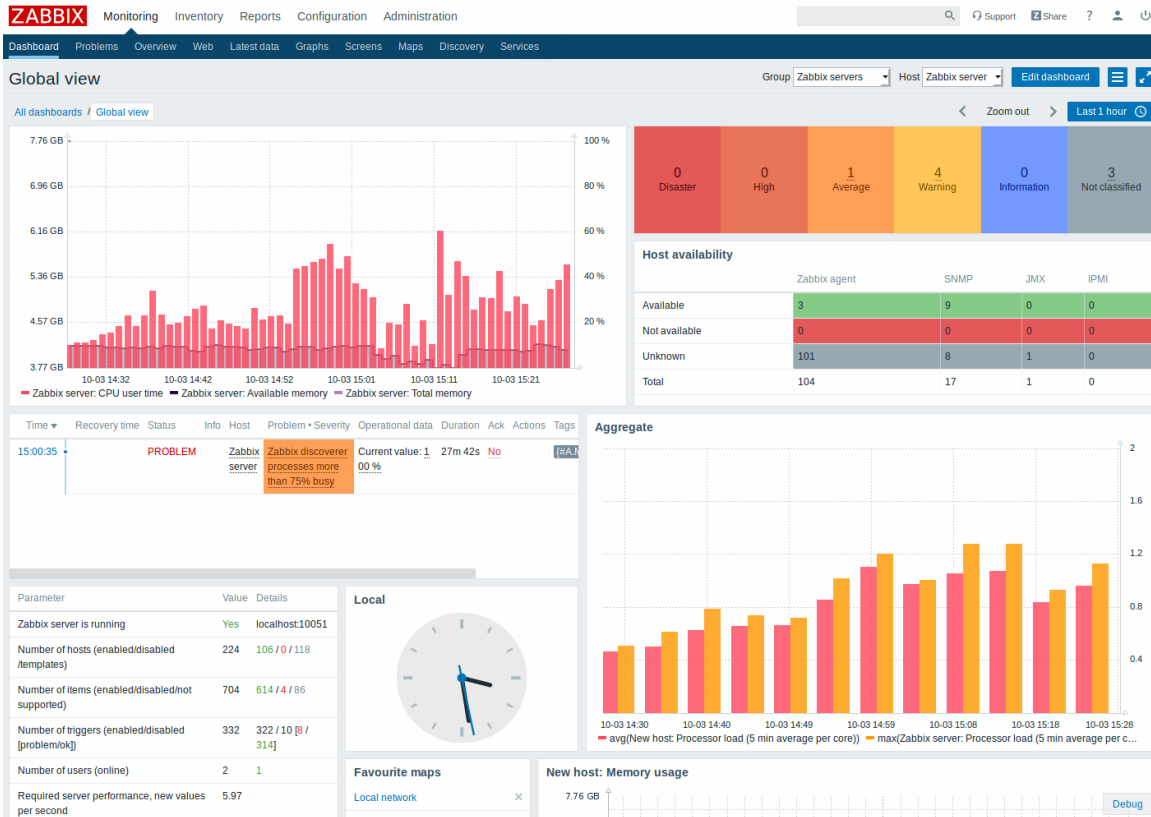


Imagen 17 Ejemplo de Dashboard en Zabbix. [Fuente zabbix.com/documentation/6.0/en/manual/web_interface/frontend_sections/monitoring/dashboard]

Tabla 39 Métrica de evaluación para Zabbix. [Fuente Propia]

Control	Criterio	¿Cuenta con el criterio?			
		No cuenta (0)	Poco (1)	Regular (2)	Totalmente (3)
A.12.1.1 Documentación de procedimientos operacionales	Existe documentación				X
	Cuenta con soporte técnico			X	
A.12.4.1 Registro de eventos	Genera reportes				X
	La información se registra y almacena				X
A.16.1.2 Notificación de los eventos de seguridad de la información	Cuenta con trigger de acciones ante eventos			X	
	Advierte de eventos o anomalías				X
A.18.1.3 Protección de los registros de la organización	La herramienta / software es segura				X
	Cuenta con respaldo			X	
Total:		21 PUNTOS			

(ZABBIX, s.f.), (ZABBIX, s.f.)

Comparación PRTG, Zabbix y WireShark

PAESSLER PRTG

Es una herramienta para el monitoreo de redes, intuitivo, fácil de manejar, fácil de instalar, en sus alcances están los protocolos ICMP, SNMP, VMI, HTTPS, OPC UA, entre muchos más.

Entre sus ventajas este software es personalizable, envía alertas en caso de errores o anomalías en la red, además de los recursos, los tiempos de uso de los dispositivos, informes, soporte técnico, etc. Sin embargo, una desventaja para situaciones u organizaciones donde no se tenga presupuesto o no se apruebe presupuesto es que la versión gratuita permite el uso de 100 sensores, cada sensor monitorea un solo aspecto de un dispositivo, por ejemplo, una URL, otro sensor para un puerto, otro sensor para el ancho de banda, así consecutivamente.

Otra cualidad es que PRTG no necesita agentes para monitorear las redes, está enfocado en el

uso de sensores, los cuales en la página oficial propiedad de PAESSLER, está documentada en manuales de uso las propiedades, descripción, tutoriales, errores, entre otros aspectos relacionados a sus sensores:

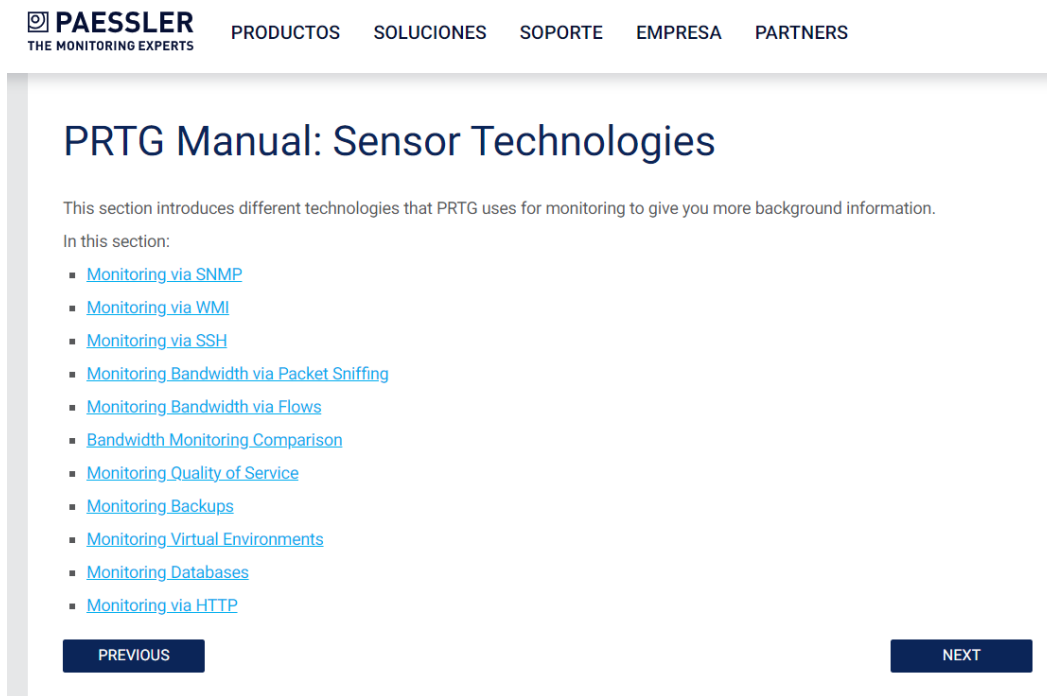


Imagen 18 Breve manual acerca de los sensores en PRTG. [Fuente paessler.com/manuals/prtg/sensor_technologies]

Buena presentación y basta pero breve información liberada al público sobre cada elemento con el que trabaja.

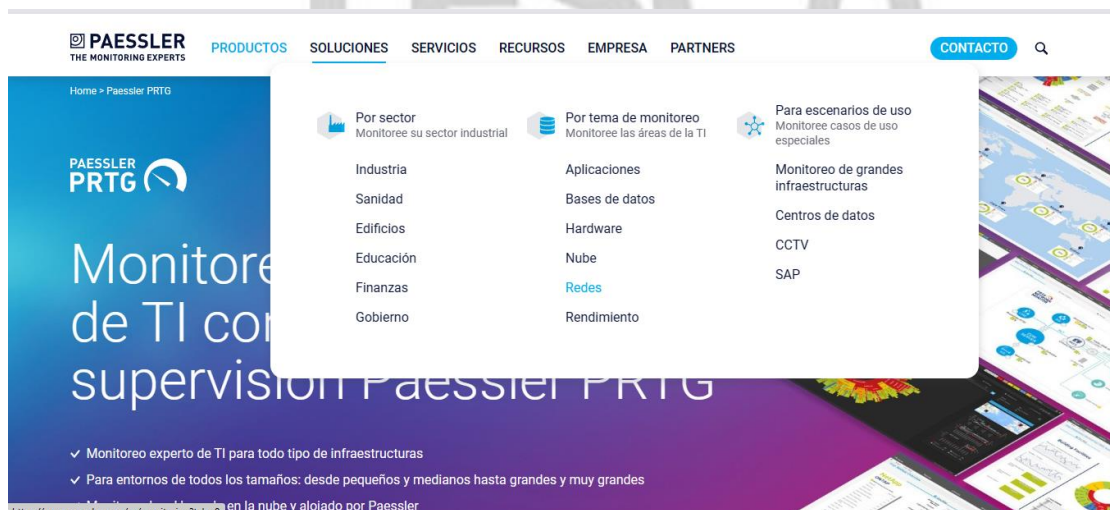


Imagen 19 Página principal de PRTG PAESSLER. [Fuente paessler.com/prtg/prtg-network-monitor]



Imagen 20 Sección Soluciones en redes de PRTG en página web. [Fuente [paessler.com/monitoring?tab=9](https://www.paessler.com/monitoring?tab=9)]



Imagen 21 Resumen de los temas de supervisión de software de red. [Fuente [paessler.com/monitoring?tab=9](https://www.paessler.com/monitoring?tab=9)]

Tabla 40 Tabla comparativa entre PRTG, Zabbix y WireShark. [Fuente Propia]

Tabla Comparativa			
Criterio	PRTG	Zabbix	WireShark
Buena presentación	Este cumple con una muy buena presentación, tanto en software como en su página oficial, contando con demasiadas secciones hablando del mismo tema, siempre a un cierto límite de divulgación	Su presentación es buena, no tan comercial como PRTG, es más moderada en su página web y software. Al ser un software gratuito, muestra su manual e información fácilmente.	La presentación es modesta, sencilla, pero a pesar de ser software gratuito su documentación es escasa. El software igualmente cumple con su función, sin embargo, no tiene la amigabilidad con el usuario.
Utilidad	Es un software comercial, ha sido creado para monitorear muchos elementos de la red y sus dispositivos, triggers, acciones, alarmas y bien representados lógicamente y estéticamente.	Zabbix cuenta con plantillas las cuales tienen por defecto parámetros a monitorear de un equipo. Es fácil de comprender y usar. Es conlimgenble para los parámetros a monitorear, pero no es tan estético como prtg	Es una herramienta muy útil para capturar paquetes de tráfico en la red. La desventaja comparando con zabbix y prtg es la falta de triggers, plus de monitoreo en otros elementos de los dispositivos, no cuenta con avanzada interfaz gráfica de usuario y no se hacen reportes
Escalabilidad	Muy escalable por el hecho de todas las funciones que puede monitorear y toma de acciones	Muy escalable, zabbix es de código abierto, puede configurarse los propios parámetros sobre lo que se desea monitorear	Es una poderosa herramienta para monitorear el tráfico, pero fuera de ello no cuenta con escalabilidad
Cumple con los requerimientos de la empresa	Solamente cumple en el uso de no agentes y la amplia gama de elementos a monitorear	Es gratuito, escalable, pero necesita agentes u otras funciones para monitorear más allá del ICMP	No cumple con los requerimientos de la empresa
Licencia	Paga, solo permite 100 sensores de prueba	Gratuita, no tiene límites de elementos a monitorear	Gratuita
Limites	100 sensores y periodos de prueba	-	Solo se limita al tráfico de la red y paquetes de información, información muy útil pero la empresa necesita otro tipo de software

Conclusión

Zabbix es una herramienta de software equilibrado a comparación de las demás opciones. Cuenta con una breve pero amplia documentación, diferentes maneras de utilizar y descargar, con una interfaz de usuario amigable, mayor facilidad de uso e interpretación y gratuita sin límite a censores.



TESCo

4.1.2. ACTIVIDAD A REALIZAR

3.2.- Definir la configuración del servidor y de zabbix para su instalación

DESCRIPCIÓN DE LA ACTIVIDAD

Conocer los requisitos, pre-requerimientos, herramientas o softwares necesarios y las instrucciones para la instalación de zabbix, así como su configuración y la del sistema operativo CentOS.

RESULTADO DE LA ACTIVIDAD

Instrucciones de instalación

Requisitos de instalación Zabbix

La documentación del software Zabbix, en apartado de requisitos, muestra tablas de elementos y software que deben de estar preinstalados para el funcionamiento del servidor.

Las siguientes tablas muestra los elementos necesarios y seleccionados previos a Zabbix versión 6.0:

Tabla 41 Pre requisitos en software para zabbix. [Fuente Propia]

Software	Versión	Comentarios
MySQL (Data base)	8.0 o posterior	
Apache server (servidor)	1.3.12 o posterior	
PHP (Interfaz)	7.2.5 o posterior – inferior a 8.0	
Libpcrc	Versiones 8.X a 10.X	Necesaria para Perl (descripción en requisitos Apache)
Libevent		Requerido para soporte de métricas masivas y monitoreo de IPMI. Versión 1.4 o superior. Tenga en cuenta que para el proxy Zabbix este requisito es opcional; es necesario para el soporte de monitoreo de IPMI.
Libpthread		Dar soporte de bloqueo de lectura y escritura
zlib		Soporte de compresión

Tabla 42 Pre requisitos en hardware para zabbix y hardware proporcionado. [Fuente Propia]

Hardware Zabbix		
Hardware	Característica	Comentarios
Memoria en RAM	128 MB mínimo	La cantidad de memoria depende de la cantidad de equipos y aspectos a monitorear
Espacio en disco	256 MB mínimo	La cantidad de memoria depende de la cantidad de equipos y aspectos a monitorear
Procesador	Virtual appliance o 2 cores/2GB	Se opta por usar un procesador virtual o como mínimo 2 núcleos de 1gb cada uno de procesamiento, esto para CentOS
Hardware proporcionado		
Hardware	Característica	Comentarios
Memoria en RAM	8 GB	
Espacio en disco	6 GB	
Procesador	4 núcleos	AMD Ryzen 5 PRO 3400G

Puertos

Los puertos por defecto que deberían ser abiertos en el firewall para que Zabbix tenga permitido las comunicaciones, según su componente, son dadas en la siguiente tabla proporcionada por la documentación.

Zabbix component	Port number	Protocol	Type of connection
Zabbix agent	10050	TCP	on demand
Zabbix agent 2	10050	TCP	on demand
Zabbix server	10051	TCP	on demand
Zabbix proxy	10051	TCP	on demand
Zabbix Java gateway	10052	TCP	on demand
Zabbix web service	10053	TCP	on demand
Zabbix frontend	80	HTTP	on demand
	443	HTTPS	on demand
Zabbix trapper	10051	TCP	on demand

Imagen 22 Puertos que usa zabbix. [Fuente zabbix.com/documentation/current/es/manual/installation/requirements]

Instalación y configuración de CentOS 9 Stream como sistema operativo

La imagen ISO también puede ser obtenida de la página oficial de CentOS. Se descarga la versión 9 Stream con arquitectura x86_64.

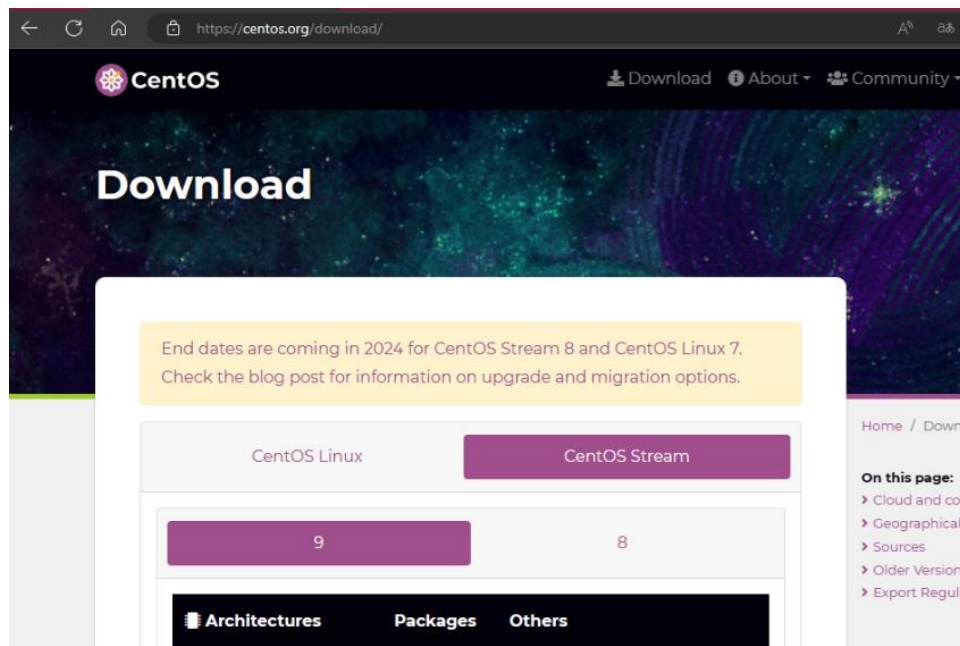


Imagen 23 Página de descarga de CentOS 9 Stream. [Fuente centos.org/download/]

TESCO

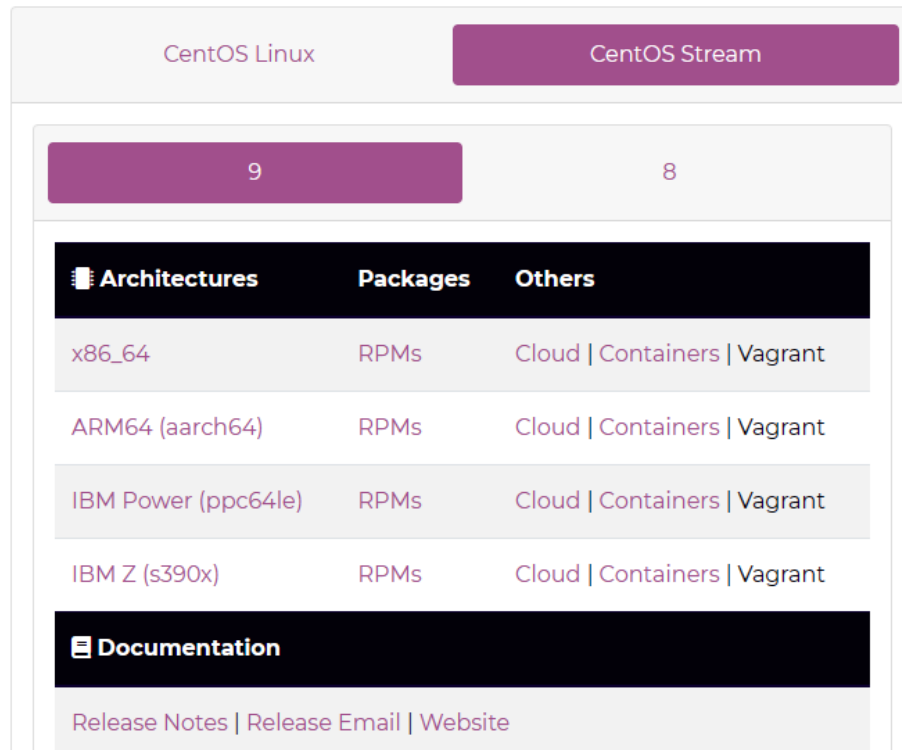


Imagen 24 Página de descarga de CentOS 9 Stream imagen 2. [Fuente centos.org/download/]

Bootear una USB con Balena Etcher con centos 9 stream o con Rufus en Windows. Para este caso en específico, se usó Rufus en un ordenador Windows para convertir en boot la usb con el sistema operativo CentOS 9 Stream.

Después de cargar el S.O. en la USB, se conecta al ordenador designado para el servidor. Se enciende y comienza a instalar centos. La primera interfaz mostrada es la siguiente:

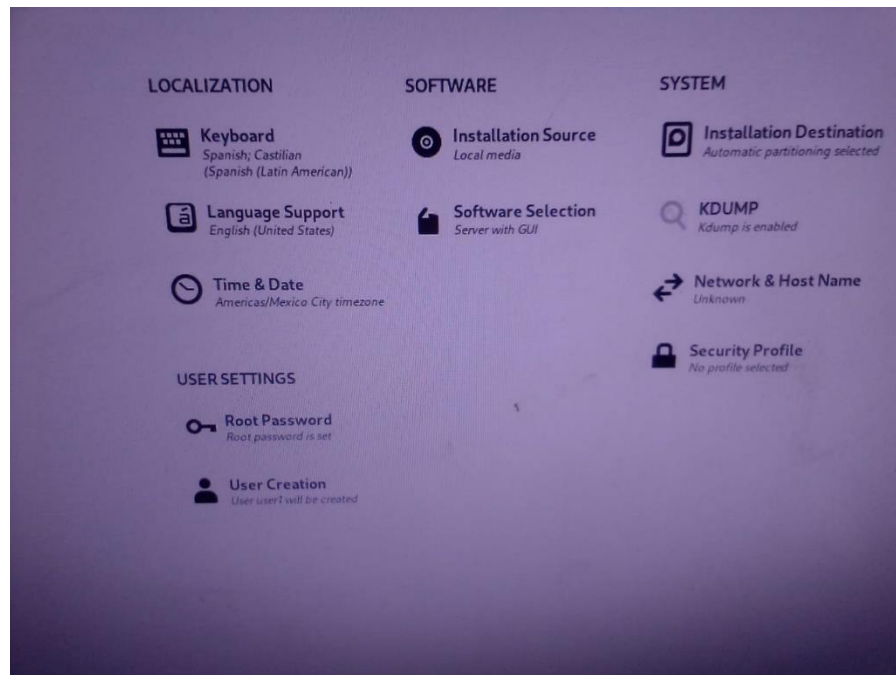


Imagen 25 Configuración de CentOS pre instalación. [Fuente Propia]

Se configuran las siguientes características:

Keyboard: a español latino america

Time & Date: Americas/Mexico City

Lenguaje: Español o Ingles

Installation destination: Elegir el disco duro donde se instalará el sistema operativo

Software Selection: Complementos y herramientas de software que pueden instalarse y dar más funciones al sistema operativo

Root password: La contraseña del administrador o super usuario

User creation: Creación y contraseña del usuario por defecto

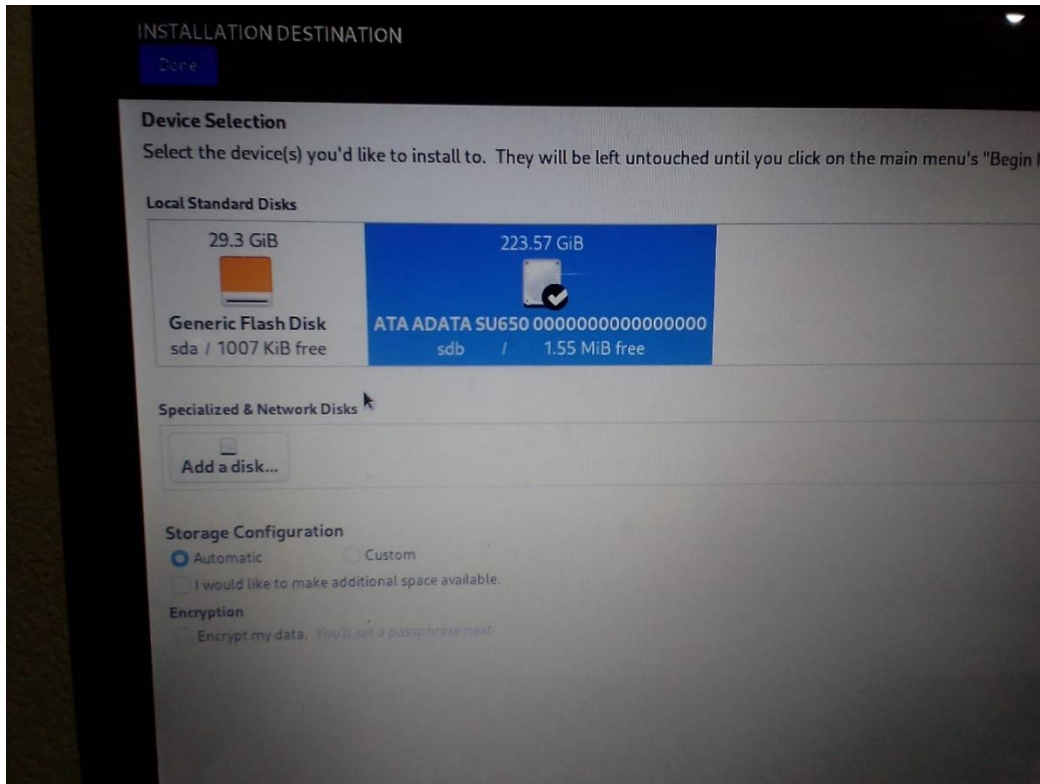


Imagen 26 Destino de instalación de CentOS pre instalación. [Fuente Propia]

Selección de software en “Software Selection”, la opción Server with GUI ayudara a visualizar

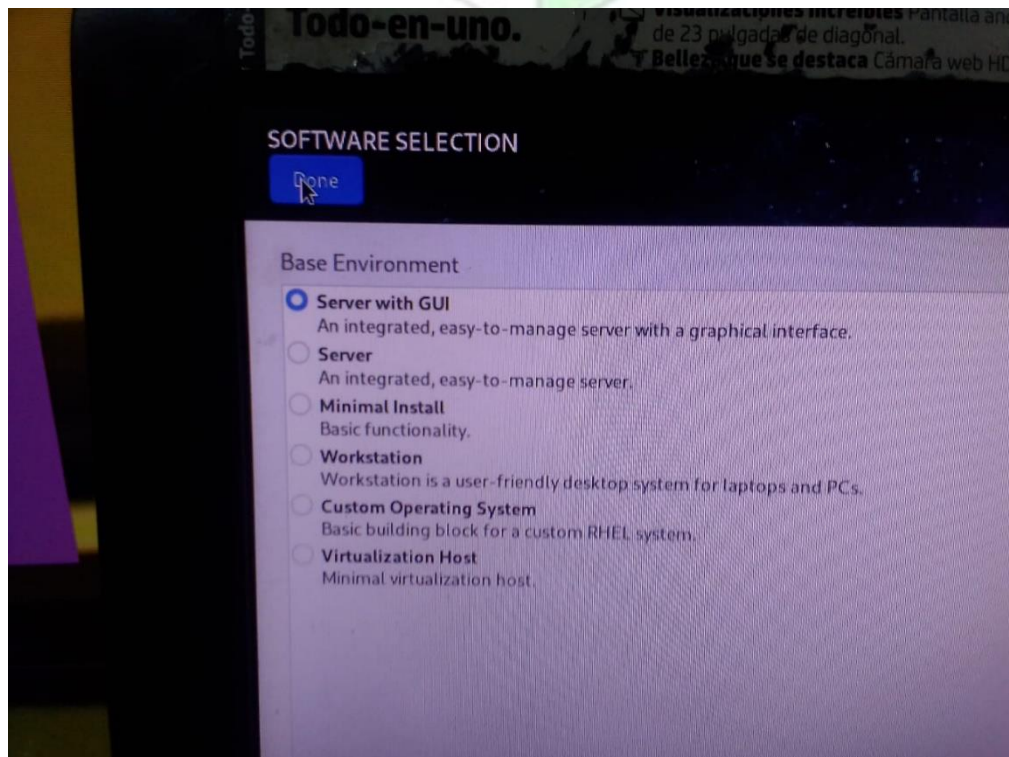


Imagen 27 Selección de software de CentOS pre instalación. [Fuente Propia]

con interfaz de usuario a zabbix a través del servidor web. Esto es útil para representar gráficas, reportes y facilitar en general vistas y acciones a tomar/configurar:

Marcar la opción de Development Tools ayudara a incluir el compilador GCC, pre-requisito para instalar Zabbix y Apache Server.

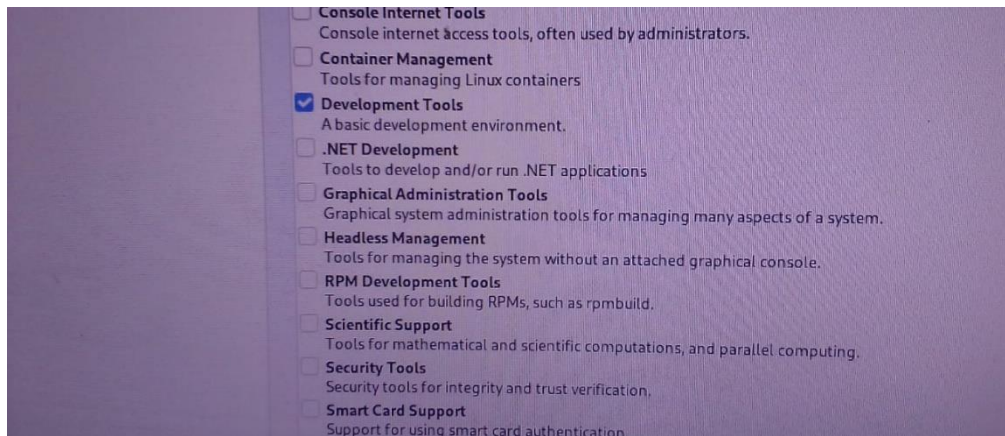


Imagen 28 Selección de software de CentOS pre instalación imagen 2. [Fuente Propia]

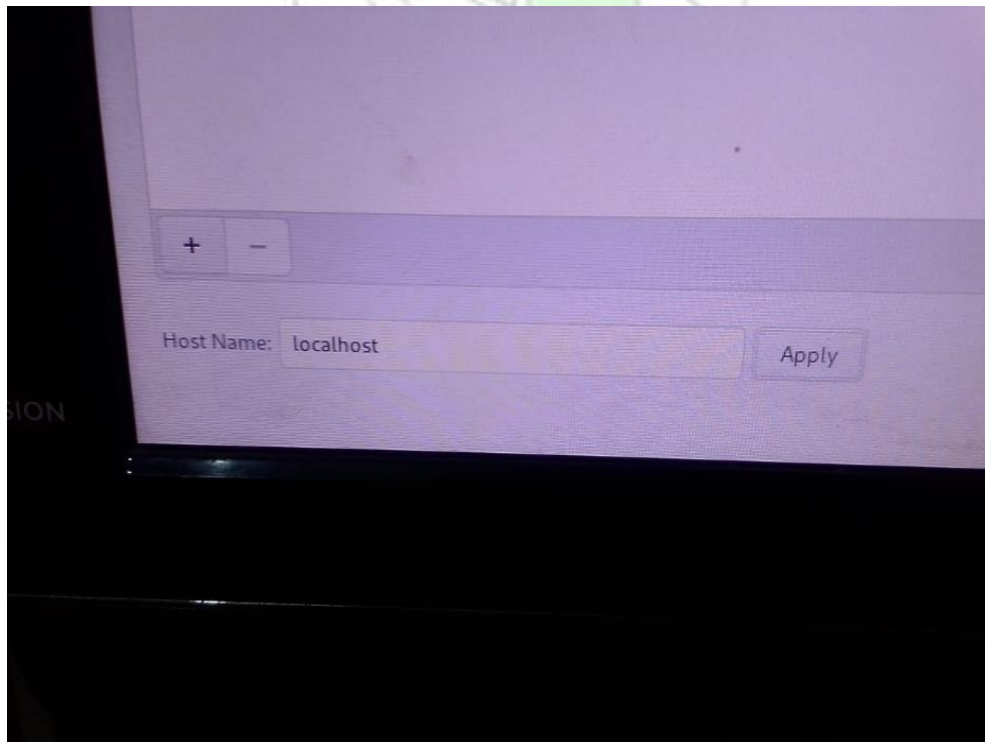


Imagen 29 Host Name para CentOS. [Fuente Propia]

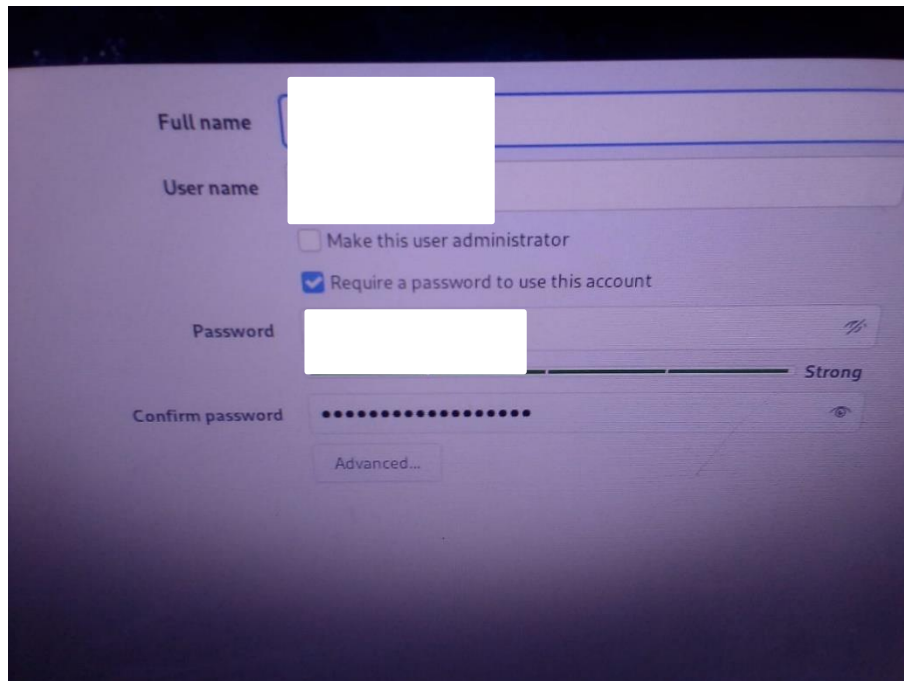


Imagen 30 Asignación de usuario normal para CentOS. [Fuente Propia]

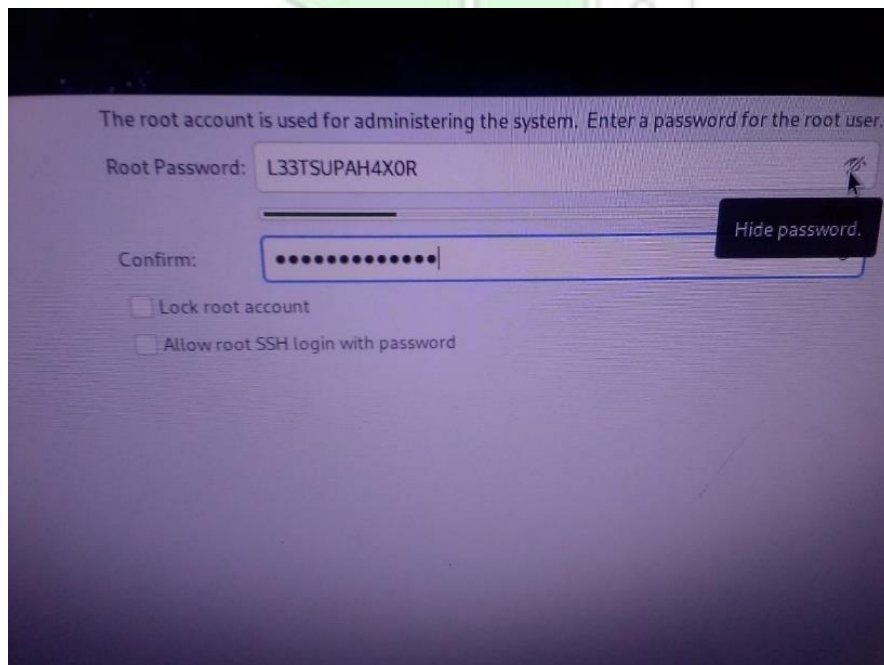


Imagen 31 Asignación de usuario root para CentOS. [Fuente Propia]

Instalación de Software y Herramientas previas a Zabbix

Para actualizar yum, debe ejecutarse el siguiente comando:

```
# yum update
```

La razón de actualizar yum es para tener a disposición al momento de instalar cualquier programa, librería o herramienta, las versiones o modificaciones más recientes.

Requisitos de Instalación de Apache server

Antes de comenzar la instalación de Apache server, debe instalarse herramientas y complementos.

Tabla 43 Requisitos para compilar Apache. [Fuente Propia]

Software/Herramienta	Descripción
APR y APR-Util	Librerías de componentes necesarios para la comunicación de otros componentes, protocolos para compilar Apache server.
Perl(PCRE)	Librería que contiene expresiones regulares (cadenas de caracteres para describir o encontrar patrones)
Espacio en disco	50 MB mínimo
Sistema de compilación ANSI-C	Compilador GNU C (GCC) como herramienta para compilar apache a través de comando como make
Ajuste exacto del sistema	Es necesario para mantener sincronizado la hora y el día con el protocolo HTTP para cualquier instalación o actualización

Instalar GCC

Para facilitar la instalación del compilador GCC y añadir sus componentes, en la página oficial de Red Hat, se pueden encontrar dos formas de instalar GNU GCC:

Tabla 44 Formas de instalar GCC. [Fuente Propia]

Sección	Comando	Página
1.5.1. Installing All Available Components - Table 1.1. Red Hat Developer Toolset Components - Chapter 1. Red Hat Developer Toolset	yum install devtoolset-6	access.redhat.com/documentation/es-es/red_hat_developer_toolset/6/html/user_guide/sect-red_hat_developer_toolset-install
Aportes de la comunidad	sudo yum group install "Development Tools"	access.redhat.com/discussions/6972672

Es posible verificar la versión de GCC con los comandos:

```
which gcc
```

```
gcc -v
```

Nota: Al instalar el sistema operativo de CentOS, al elegir el tipo de interfaz y sus componentes, el seleccionar “Development Tools” ya no es necesario instalar GCC, ya que se instala con esta propiedad.

Instalar expat

Es necesario para la instalación de APR-UTIL. En la página oficial de Apache “apr.apache.org” en la sección para descargar APR-Util “Apache Portable Runtime Utility 1.6.3 Released” existe un enlace con nombre “CHANGES-APR-UTIL-1.6” la cual redirige a la siguiente dirección “downloads.apache.org/apr/CHANGES-APR-UTIL-1.6” y encontramos la siguiente consideración:

changes with APR-util 1.6.0

*) The expat dependency of apr-util is no longer built with apr-util.
Install expat (including development headers and libraries) first
before building apr-util. [<https://libexpat.github.io/>]

Imagen 32 Cambios en APR-util versión 1.6.0 o superior. [Fuente downloads.apache.org/apr/CHANGES-APR-UTIL-1.6]

Descargar de github.com/libexpat/libexpat/releases y ejecutar los siguientes comandos:

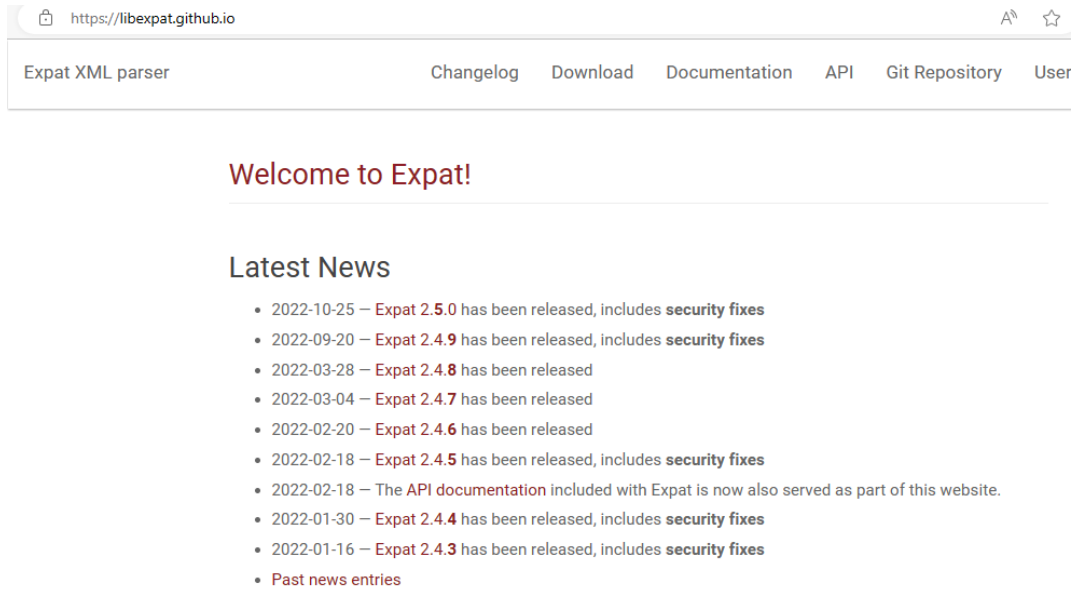


Imagen 33 Página para la descarga de expat. [Fuente libexpat.github.io]

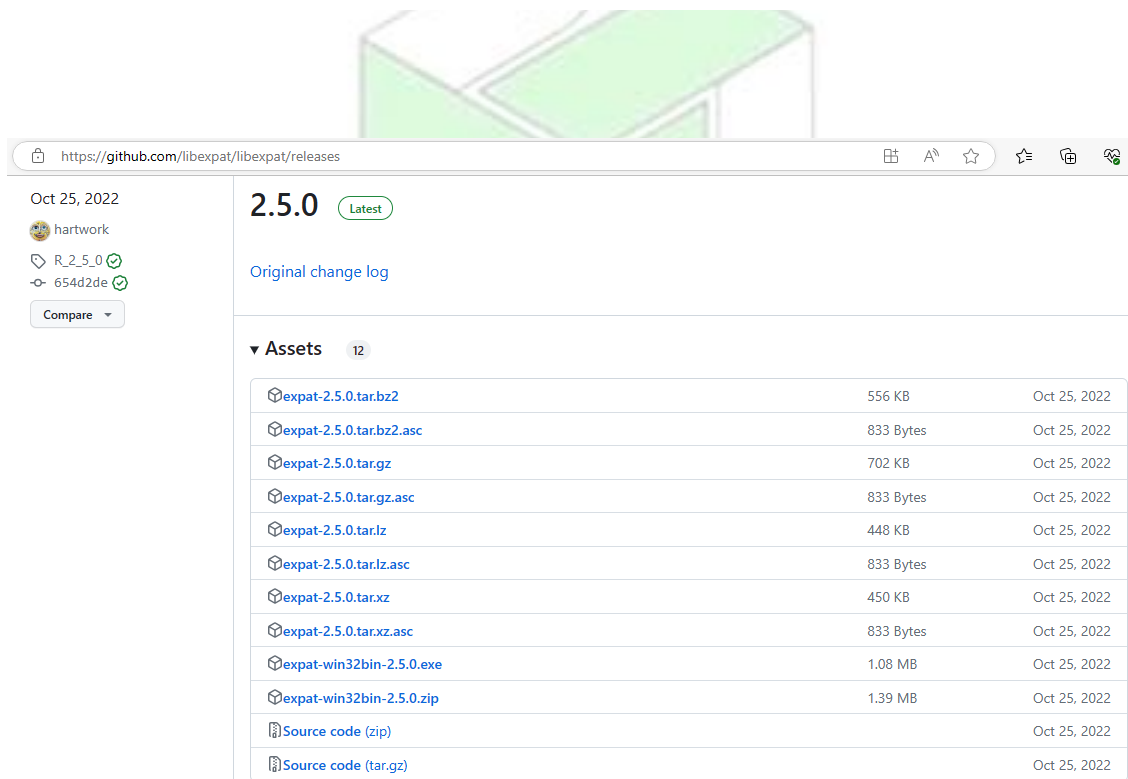


Imagen 34 Repositorio para la descarga de expat. [Fuente github.com/libexpat/libexpat/releases]

gzip -d archivo.tar.gz

tar xvf archivo.tar

y para instalar, entrar a la carpeta y ejecutar:

./configure

make

make install

Instalar PCRE 2-10.42

Descargar la librería de github.com/PCRE2Project/pcre2/releases y ejecutar los comandos para descomprimir:

gzip -d archivo.tar.gz

tar xvf archivo.tar

y para instalar, entrar a la carpeta y ejecutar:

./configure

make

make install



← ↻ 🔒 <https://www.pcre.org>

PCRE - Perl Compatible Regular Expressions

The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as the POSIX regular expression API. The PCRE library is free, even for building proprietary software.

PCRE was originally written for the [Exim MTA](#), but is now used by many high-profile open source projects, including [Apache](#) products, like [Apple Safari](#). Some other interesting projects using PCRE include [Chicken](#), [Onyx](#), [Hypermail](#), [Leafnode](#), [Asterisk](#).

Versions

There are two major versions of the PCRE library. The current version, PCRE2, [released in 2015](#), is now at version **10.39**.

The older, but still widely deployed PCRE library, originally released in 1997, is at version **8.45**. This version of PCRE is the release of the older PCRE library, and new projects should use PCRE2 instead.

Download

You can download the current release of the PCRE2 library from its official home on [GitHub](#):

- <https://github.com/PhilipHazel/pcre2/releases>

Imagen 35 Página para la descarga de PCRE. [Fuente pcre.org]

Nota: De no instalar esta librería, el error se arrojará al intentar instalar Apache, similar al

siguiente:
configure: error: pcre-config para libpcre no encontrado

Instalar APR 1.7.4

Descargar APR desde la página oficial de Apache “apr.apache.org”.

Apache Portable Runtime 1.7.4 Released

The Apache Software Foundation and the Apache Portable Runtime Project are proud to announce the General Availability of version 1.7.4 of the Apache Portable Runtime library. APR 1.7 brings a number of enhancements and bugfixes documented in [CHANGES](#). Users of earlier versions are encouraged to update to this release.

For further details of this release, see the [official announcement](#) as well as the [CHANGES-APR-1.7](#) file.

[Download](#)

Programmer's Manual: [APR](#)

Imagen 36 Página para la descarga de APR 1.7.4. [Fuente apr.apache.org]

Elegir la opción de archivo.tar.gz.

APR 1.7.4 is the best available version

APR is the base portability library.

- Unix Source: [apr-1.7.4.tar.gz](#) [[PGP](#)] [[SHA256](#)]
- Unix Source: [apr-1.7.4.tar.bz2](#) [[PGP](#)] [[SHA256](#)]
- Win32 Source: [apr-1.7.4-win32-src.zip](#) [[PGP](#)] [[SHA256](#)]
- [Other files](#)

Imagen 37 Sección para la descarga de APR 1.7.4. [Fuente apr.apache.org]

Ejecutar los comandos para descomprimir:

`gzip -d archivo.tar.gz`

`tar xvf archivo.tar`

y para instalar, entrar a la carpeta y ejecutar:

`./configure`

`make`

`make install`

Instalar APR-Util 1.6.3

Descargar APR-Util desde la página oficial de Apache “apr.apache.org”.

Apache Portable Runtime Utility 1.6.3 Released

The Apache Software Foundation and the Apache Portable Runtime Project are proud to announce the General Availability of version 1.6.3 of the APR Apache Portable Runtime Utility library. Users of earlier versions are encouraged to update to this release.

The main changes in this release are concerned with the third-party dependencies, including unbundling expat, and building with up-to-date versions of libraries such as OpenSSL and MySQL.

For further details of this release, see the [official announcement](#) as well as the [CHANGES-APR-UTIL-1.6](#) file.

[Download](#)

Programmer's Manual: [APR-util](#)

Imagen 38 Página para la descarga de APR Util 1.6.3. [Fuente apr.apache.org]

Elegir la opción de archivo.tar.gz.

APR-util 1.6.3 is the best available version

APR-util provides a number of helpful abstractions on top of APR.

- Unix Source: [apr-util-1.6.3.tar.gz](#) [PGP] [SHA256]
- Unix Source: [apr-util-1.6.3.tar.bz2](#) [PGP] [SHA256]
- Windows Source: [apr-util-1.6.3-win32-src.zip](#) [PGP] [SHA256]
- [Other files](#)

Imagen 39 Sección para la descarga de APR Util 1.6.3. [Fuente apr.apache.org]

Ejecutar los comandos para descomprimir:

```
gzip -d archivo.tar.gz
```

```
tar xvf archivo.tar
```

y para instalar, entrar a la carpeta y ejecutar:

```
./configure --with-apr=/usr/local/apr/bin/apr-1-config
```

```
make
```

```
make install
```

--with-apr es la dirección de un archivo de configuración de APR que necesita APR-Util. Al intentar ejecutar únicamente “./configure” en APR-Util, al finalizar mostrara un error en la terminar acompañado de la solución la cual debe de indicarse la dirección “/usr/local/apr/bin/apr-1-config”.

Instalar Apache Server

En Apache y la página web de PHP se encuentran 3 maneras de instalar Apache

Tabla 45 Maneras de instalar PHP. [Fuente Propia]

Web Site	Comando
Apache.org	sudo yum install httpd
Apache.org	Download the latest release from http://httpd.apache.org/download.cgi Extract \$ gzip -d httpd-NN.tar.gz \$ tar xvf httpd-NN.tar \$ cd httpd-NN Configure \$./configure --prefix=PREFIX Compile \$ make Install \$ make install Customize \$ vi PREFIX/conf/httpd.conf Test \$ PREFIX/bin/apachectl -k start PREFIX es comúnmente /usr/local/apache2
PHP	tar -xzf httpd-2.x.NN.tar.gz cd httpd-2_x_NN ./configure --enable-so make make install

La opción recomendada es desde la página oficial de Apache e instalando desde el archivo.tar.gz descargable de “httpd.apache.org/download.cgi#apache24”.

Instalación de MySQL

Descargar e instalar el Mysql community reléase. Este es un repositorio de mysql, quiere decir que contendrá archivos que serán necesarios para el funcionamiento de mysql server.

Descargar de “dev.mysql.com/downloads/repo/yum/” el archivo para Red Hat Enterprise

Linux 9.

MySQL Community Downloads

MySQL Yum Repository



Imagen 40 Descarga de MySQL Community oficial. [Fuente dev.mysql.com/downloads/repo/yum/]

Ejecutar los comandos para instalar:

```
$> sudo yum install mysql80-community-release-el9-{version-number}.noarch.rpm
```

El siguiente comando habilita y muestra que el repositorio de MySQL se haya añadido:

```
$> yum repolist enabled | grep "mysql.*-community.*"
```

Instalar MySQL por medio del siguiente comando:

```
$> sudo yum install mysql-community-server
```

Inicia el servidor con el siguiente comando:

```
$> systemctl start mysqld
```

El usuario root de MySQL tendrá una contraseña temporal, la cual debe cambiarse una vez ingrese al servidor.

Primero ingresar el siguiente código para obtener la contraseña:

```
$> sudo grep 'temporary password' /var/log/mysqld.log
```

Ingresa al servidor de mysql:

```
$> mysql -uroot -p
```

Cambia la contraseña colocando la nueva en lugar de MyNewPass4!:

```
mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 'MyNewPass4!';
```

Nota: En caso de mostrar la terminal un error sobre la librería libxml2-devel faltante, se puede instalar con el comando: `yum install libxml2-devel`

Instalación PHP

Descargar de php.net/releases/ la versión deseada, en este caso basado en los requerimientos de Zabbix Server V6.0 la versión de PHP debe ser V7.2.5 o superior e inferior a 8.0. La opción elegida es la Versión V7.3.33

Descomprime y ejecuta para instalar:

```
cd ../php-NN
```

```
./configure --with-apxs2=/usr/local/apache2/bin/apxs --with-pdo-mysql
```

```
make
```

```
make install
```

Instalar y configurar Zabbix

Escoger la versión a instalar de Zabbix. S.O., componentes, base de datos y web server. Se ha elegido la versión V6.0, es una versión anterior a la más actual, la documentación de la instalación de Zabbix se encuentra en su página oficial, en el ítem del menú principal “PRODUCT - Download and install Zabbix”.

Download and install Zabbix

Zabbix
PackagesZabbix
Cloud
ImagesZabbix
ContainersZabbix
ApplianceZabbix
SourcesZabbix
Agents

1

Choose your platform

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER
6.4	Alma Linux	9 Stream	Server, Frontend, Agent	MySQL	Apache
6.0 LTS	CentOS	8 Stream	Proxy	PostgreSQL	Nginx
5.0 LTS	Debian	7	Agent		
4.0 LTS	Oracle Linux	6	Agent 2		

Imagen 41 Sección descarga de Zabbix. [Fuente zabbix.com/download]

Instalar el repositorio de Zabbix:

```
# rpm -Uvh https://repo.zabbix.com/zabbix/6.0/rhel/9/x86_64/zabbix-release-6.0-4.el9.noarch.rpm
```

```
# dnf clean all
```

Instalar Zabbix server, frontend y agente

```
# dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent
```

Crear una base de datos para Zabbix en MySQL

```
# mysql -uroot -p
```

```
password
```

```
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
```

```
mysql> create user zabbix@localhost identified by 'password';
```

```
mysql> grant all privileges on zabbix.* to zabbix@localhost;
```

```
mysql> set global log_bin_trust_function_creators = 1;
```

```
mysql> quit;
```

Importar al host del servidor de zabbix el esquema y los datos

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Deshabilitar log_bin_trust_function_creators

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

Configurar la base de datos para Zabbix Server entrando a la siguiente dirección y editando el archivo: /etc/zabbix/zabbix_server.conf

Edita la siguiente sentencia con la contraseña establecida para el usuario en la base de datos de zabbix. El usuario es zabbix@localhost:

DBPassword=password

Iniciar Zabbix Server y el proceso de agente

```
# systemctl restart zabbix-server zabbix-agent httpd php-fpm
# systemctl enable zabbix-server zabbix-agent httpd php-fpm
```

Entrar a Zabbix Server por web frontend, existen tres opciones:

- 1) http://host/zabbix
- 2) localhost/zabbix
- 3) dirección_ip_del_ordenador/zabbix

Ingresa al web de zabbix es necesario entrar con usuario: Admin

Contraseña: zabbix

4.1.3. ACTIVIDAD A REALIZAR

3.3.- Implementar el servidor en la red local

DESCRIPCIÓN DE LA ACTIVIDAD

Siguiendo las instrucciones y requisitos establecidos en la actividad anterior, instala e implementa el servidor Zabbix en el equipo proporcionado por la empresa.

RESULTADO DE LA ACTIVIDAD

Tabla 46 Hardware proporcionado por la empresa. [Fuente Propia]

Hardware proporcionado		
Hardware	Característica	Comentarios
Memoria en RAM	8 GB	
Espacio en disco	6 GB	
Procesador	4 núcleos	AMD Ryzen 5 PRO 3400G
Modelo	Computadora de escritorio Lenovo ThinkCentre	
Fotografía		
		

Implementación y configuración de servidor Zabbix en el monitoreo de la intranet local

Se realizó la configuración del sistema CentOS como se explica en la actividad 3.2.- **Definir la configuración del servidor y de zabbix para su instalación.**

Resumen de la configuración:

Keyboard: a español latino america

Time & Date: Americas/Mexico City

Lenguaje: Español o Inglés

Installation destination: Elegir el disco duro donde se instalará el sistema operativo

Software Selection: Complementos y herramientas de software que pueden instalarse y dar más funciones al sistema operativo

Root password: La contraseña del administrador o super usuario

User creation: Creación y contraseña del usuario por defecto

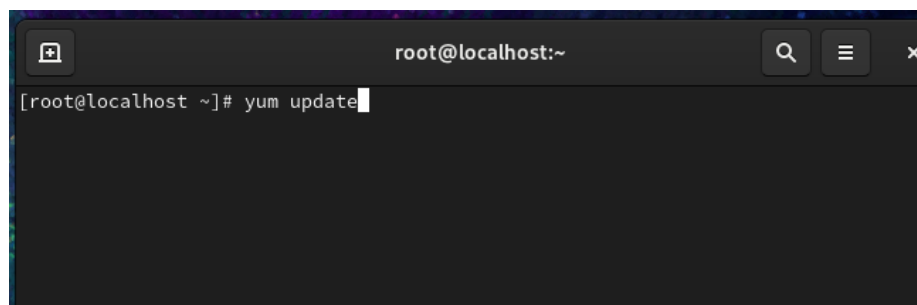
Después de ingresar como usuario root en CentOS, seguir las instrucciones de instalación y pre-requisitos de software para zabbix.

Actualizar yum

Para actualizar yum, debe ejecutarse el siguiente comando:

```
# yum update
```

La razón de actualizar yum es para tener a disposición al momento de instalar cualquier programa, librería o herramienta, las versiones o modificaciones más recientes.



```
root@localhost:~  
[root@localhost ~]# yum update
```

Imagen 42 Actualización de yum. [Fuente Propia]

```

root@localhost:~
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing                : 1/1
  Upgrading                : libtiff-4.4.0-8.el9.x86_64 1/6
  Upgrading                : efi-srpm-macros-4-9.el9.noarch 2/6
  Upgrading                : efi-filesystem-4-9.el9.noarch 3/6
  Cleanup                  : efi-srpm-macros-4-8.el9.noarch 4/6
  Cleanup                  : efi-filesystem-4-8.el9.noarch 5/6
  Cleanup                  : libtiff-4.4.0-7.el9.x86_64 6/6
  Running scriptlet: libtiff-4.4.0-7.el9.x86_64 6/6
  Verifying                : efi-filesystem-4-9.el9.noarch 1/6
  Verifying                : efi-filesystem-4-8.el9.noarch 2/6
  Verifying                : efi-srpm-macros-4-9.el9.noarch 3/6
  Verifying                : efi-srpm-macros-4-8.el9.noarch 4/6
  Verifying                : libtiff-4.4.0-8.el9.x86_64 5/6
  Verifying                : libtiff-4.4.0-7.el9.x86_64 6/6

Upgraded:
  efi-filesystem-4-9.el9.noarch      efi-srpm-macros-4-9.el9.noarch
  libtiff-4.4.0-8.el9.x86_64

Complete!
[root@localhost ~]#

```

Imagen 43 yum actualizado. [Fuente Propia]

Instalación de GCC

Para facilitar la instalación del compilador GCC y añadir sus componentes, en la página oficial de Red Hat, se pueden encontrar dos formas de instalar GNU GCC:

Tabla 47 Maneras de instalar GCC. [Fuente Propia]

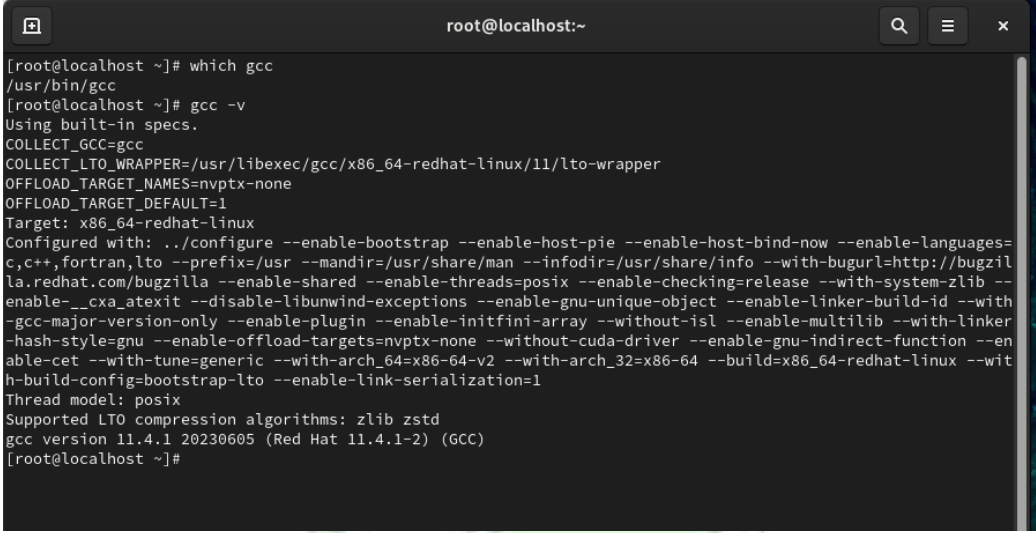
Sección	Comando	Página
1.5.1. Installing All Available Components - Table 1.1. Red Hat Developer Toolset Components - Chapter 1. Red Hat Developer Toolset	yum install devtoolset-6	access.redhat.com/documentation/es-es/red_hat_developer_toolset/6/html/user_guide/sect-red_hat_developer_toolset-install
Aportes de la comunidad	sudo yum group install "Development Tools"	access.redhat.com/discussions/6972672

Es posible verificar la versión de GCC con los comandos:

which gcc

gcc -v

Nota: Al instalar el sistema operativo de CentOS, al elegir el tipo de interfaz y sus componentes, el seleccionar “Development Tools” ya no es necesario instalar GCC, ya que se instala con esta propiedad.



```

root@localhost:~# which gcc
/usr/bin/gcc
root@localhost:~# gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Target: x86_64-redhat-linux
Configured with: ../configure --enable-bootstrap --enable-host-pie --enable-host-bind-now --enable-languages=c,c++,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=http://bugzilla.redhat.com/bugzilla --enable-shared --enable-threads=posix --enable-checking=release --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-initfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch_64=x86-64-v2 --with-arch_32=x86-64 --build=x86_64-redhat-linux --with-h-build-config=bootstrap-lto --enable-link-serialization=1
Thread model: posix
Supported LTO compression algorithms: zlib zstd
gcc version 11.4.1 20230605 (Red Hat 11.4.1-2) (GCC)
root@localhost:~#

```

Imagen 44 Instalación de GCC comprobado. [Fuente Propia]

Instalación de expat

Es necesario para la instalación de APR-UTIL. En la página oficial de Apache “apr.apache.org” en la sección para descargar APR-Util “Apache Portable Runtime Utility 1.6.3 Released” existe un enlace con nombre “CHANGES-APR-UTIL-1.6” la cual redirige a la siguiente dirección “downloads.apache.org/apr/CHANGES-APR-UTIL-1.6” y encontramos la siguiente consideración:

changes with APR-util 1.6.0

- *) The expat dependency of apr-util is no longer built with apr-util.
Install expat (including development headers and libraries) first before building apr-util. [<https://libexpat.github.io/>]

Imagen 45 Cambios en APR-util versión 1.6.0 o superior. [Fuente downloads.apache.org/apr/CHANGES-APR-UTIL-1.6]

Descargar de github.com/libexpat/libexpat/releases y ejecutar los siguientes comandos:

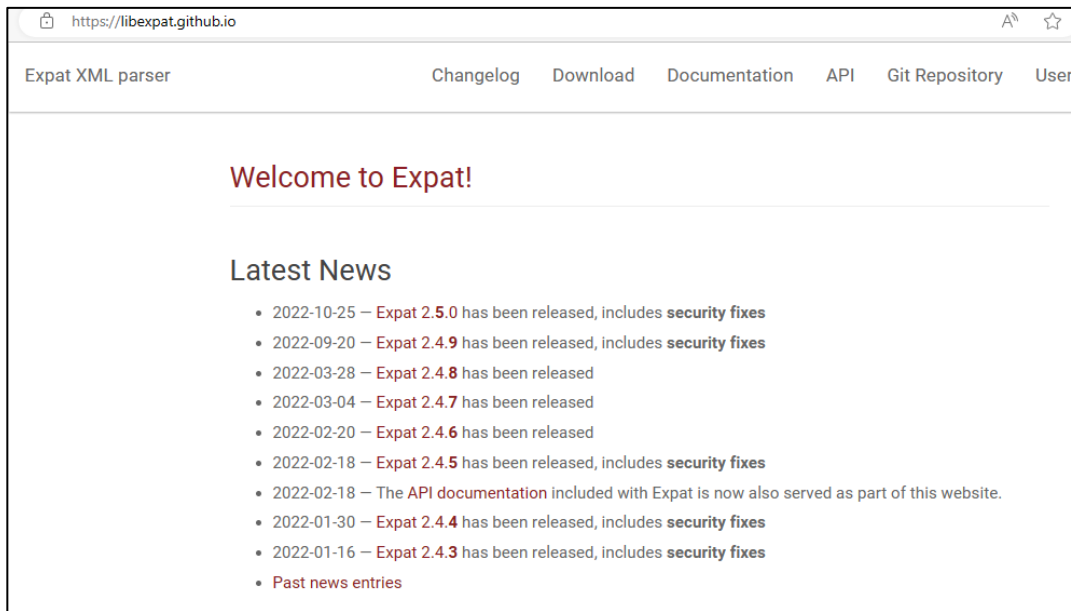


Imagen 46 Página para la descarga de expat. [Fuente libexpat.github.io]

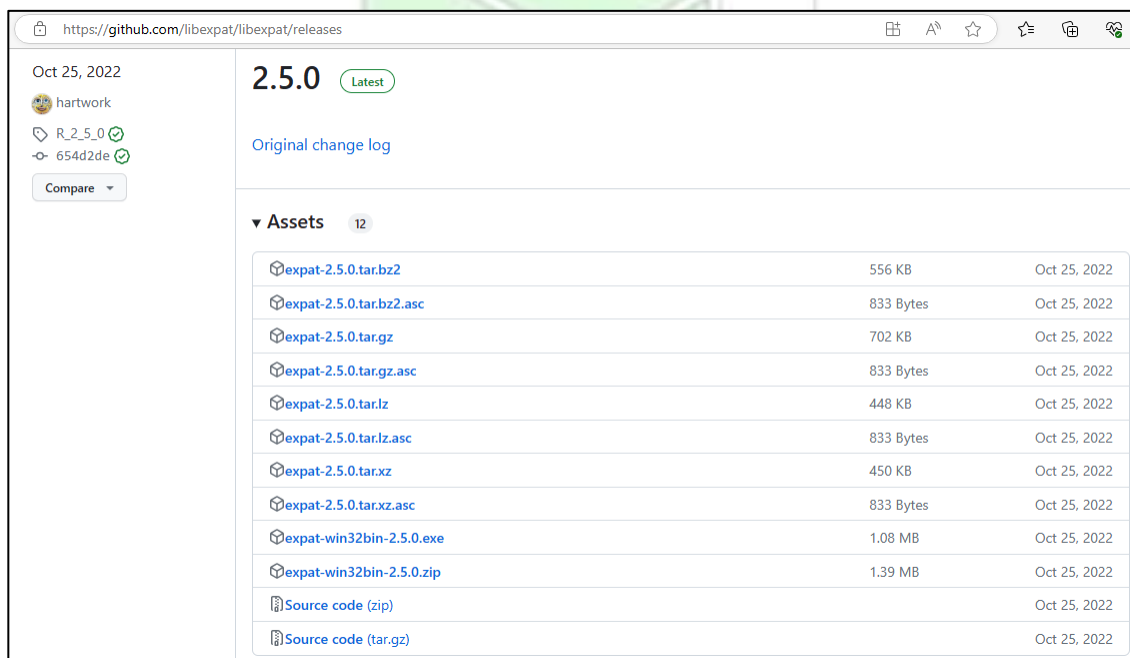


Imagen 47 Repositorio para la descarga de expat. [Fuente github.com7libexpat/libexpat/releases]

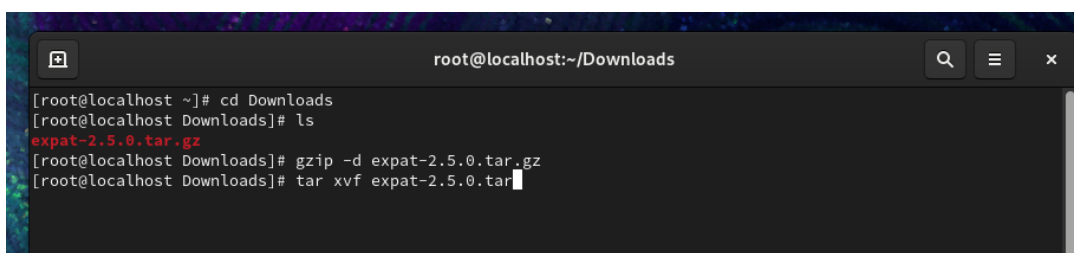


Imagen 48 Descomprimir expat. [Fuente Propia]

```
expat-2.5.0/lib/xmlrole.c
expat-2.5.0/lib/expat.h
expat-2.5.0/lib/winconfig.h
expat-2.5.0/lib/asciitab.h
expat-2.5.0/lib/xmltok.c
expat-2.5.0/lib/iasciitab.h
expat-2.5.0/lib/xmltok_ns.c
expat-2.5.0/lib/internal.h
expat-2.5.0/lib/xmlparse.c
expat-2.5.0/lib/xmltok_impl.c
expat-2.5.0/lib/ascii.h
expat-2.5.0/Changes
[root@localhost Downloads]#
[root@localhost Downloads]#
[root@localhost Downloads]#
```

Imagen 49 Expat descomprimido. [Fuente Propia]

```
root@localhost:~/Downloads/expat-2.5.0

[root@localhost Downloads]# cd expat-2.5.0/
[root@localhost expat-2.5.0]# ./configure
```

Imagen 50 Configuración en expat. [Fuente Propia]

```
config.status: creating run.sh
config.status: creating expat_config.h
config.status: executing depfiles commands
config.status: executing libtool commands
configure:

Automake flags (can be overridden by user flags):
  AM_CPPFLAGS: -DXML_ENABLE_VISIBILITY=1
  AM_CFLAGS: -Wall -Wextra -fexceptions -fno-strict-aliasing -Wmissing-prototypes -Wstrict-prototypes -pedantic -Wduplicated-cond -Wduplicated-branches -Wlogical-op -Wrestrict -Wnull-dereference -Wjump-misses-init -Wdouble-promotion -Wshadow -Wformat=2 -Wno-pedantic-ms-format -Wmisleading-indentation -fvisibility=hidden
  AM_CXXFLAGS: -Wall -Wextra -fexceptions -fno-strict-aliasing
  AM_LDFLAGS: -fno-strict-aliasing

User flags (override Automake flags on conflict):
  CPPFLAGS:
  CFLAGS: -g -O2
  CXXFLAGS: -g -O2
  LDFLAGS:
[root@localhost expat-2.5.0]# make
```

Imagen 51 Comando make en expat. [Fuente Propia]

```
codepage.o xmlwf.o unixfilemap.o ../lib/libexpat.a
libtool: link: gcc -Wall -Wextra -fexceptions -fno-strict-aliasing -Wmissing-prototypes -Wstrict-prototypes -pedantic -Wduplicated-cond -Wduplicated-branches -Wlogical-op -Wrestrict -Wnull-dereference -Wjump-misses-init -Wdouble-promotion -Wshadow -Wformat=2 -Wno-pedantic-ms-format -Wmisleading-indentation -fvisibility=hidden -g -O2 -fno-strict-aliasing -o .libs/xmlwf xmlwf-xmlwf.o xmlwf-xmlfile.o xmlwf-codepage.o xmlwf-unixfilemap.o ../lib/.libs/libexpat.so -lm -Wl,-rpath -Wl,/usr/local/lib
make[2]: Leaving directory '/root/Downloads/expat-2.5.0/xmlwf'
Making all in doc
make[2]: Entering directory '/root/Downloads/expat-2.5.0/doc'
make[2]: Nothing to be done for 'all'.
make[2]: Leaving directory '/root/Downloads/expat-2.5.0/doc'
make[2]: Entering directory '/root/Downloads/expat-2.5.0'
make[2]: Leaving directory '/root/Downloads/expat-2.5.0'
make[1]: Leaving directory '/root/Downloads/expat-2.5.0'
[root@localhost expat-2.5.0]# make install
```

Imagen 52 Comando make install en expat. [Fuente Propia]

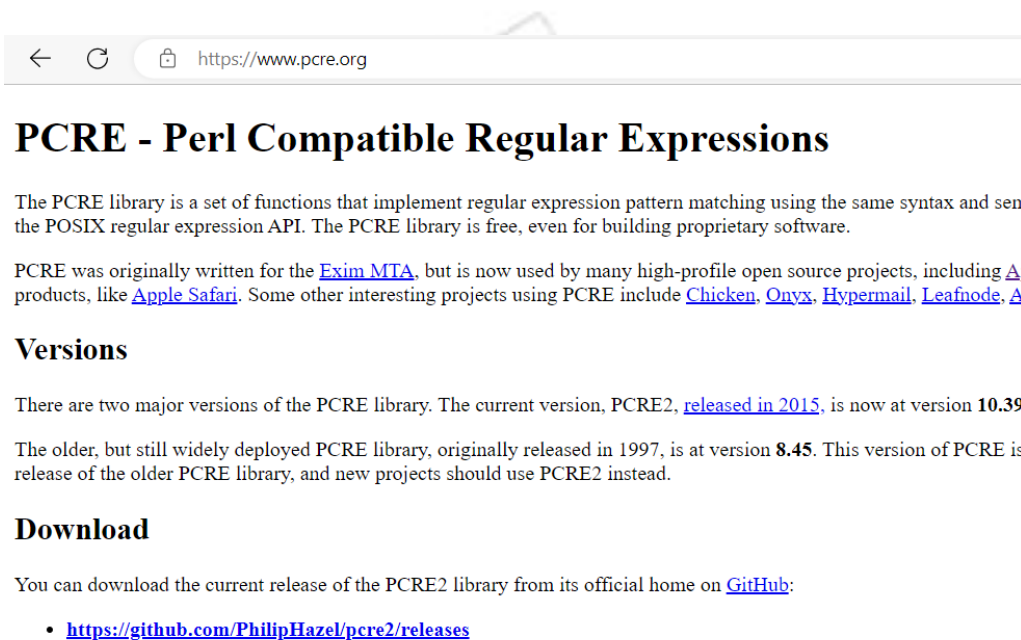
```

make[1]: Entering directory '/root/Downloads/expat-2.5.0'
make[2]: Entering directory '/root/Downloads/expat-2.5.0'
make[2]: Nothing to be done for 'install-exec-am'.
/usr/bin/mkdir -p '/usr/local/lib/cmake/expat-2.5.0'
/usr/bin/install -c -m 644 cmake/autotools/expat.cmake '/usr/local/lib/cmake/expat-2.5.0'
/usr/bin/mkdir -p '/usr/local/lib/cmake/expat-2.5.0'
/usr/bin/install -c -m 644 cmake/autotools/expat-config-version.cmake cmake/autotools/expat-noconfig.cmake c
make/expat-config.cmake '/usr/local/lib/cmake/expat-2.5.0'
/usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
/usr/bin/install -c -m 644 expat.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/root/Downloads/expat-2.5.0'
make[1]: Leaving directory '/root/Downloads/expat-2.5.0'
[root@localhost expat-2.5.0]#

```

Imagen 53 Expat instalado. [Fuente Propia]

Instalación PCRE 2-10.42



The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as the POSIX regular expression API. The PCRE library is free, even for building proprietary software.

PCRE was originally written for the [Exim MTA](#), but is now used by many high-profile open source projects, including [Apache](#) products, like [Apple Safari](#). Some other interesting projects using PCRE include [Chicken](#), [Onyx](#), [Hypermail](#), [Leafnode](#), [A](#).

Versions

There are two major versions of the PCRE library. The current version, PCRE2, [released in 2015](#), is now at version **10.39**.

The older, but still widely deployed PCRE library, originally released in 1997, is at version **8.45**. This version of PCRE is the last release of the older PCRE library, and new projects should use PCRE2 instead.

Download

You can download the current release of the PCRE2 library from its official home on [GitHub](#):

- <https://github.com/PhilipHazel/pcre2/releases>

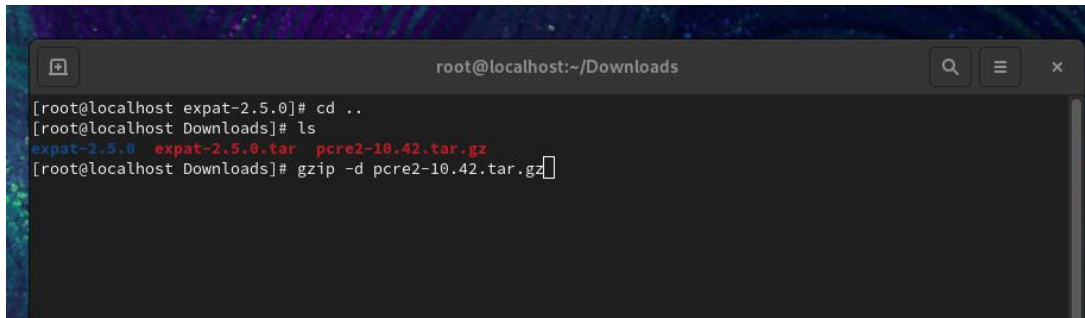
Imagen 54 Página para la descarga de PCRE. [Fuente pcre.org]

Nota: De no instalar esta librería, el error se arrojará al intentar instalar Apache, similar al siguiente:
configure: error: pcre-config para libpcre no encontrado

Descargar la librería de github.com/PCRE2Project/pcre2/releases y ejecutar los comandos para descomprimir:

gzip -d archivo.tar.gz

tar xvf archivo.tar

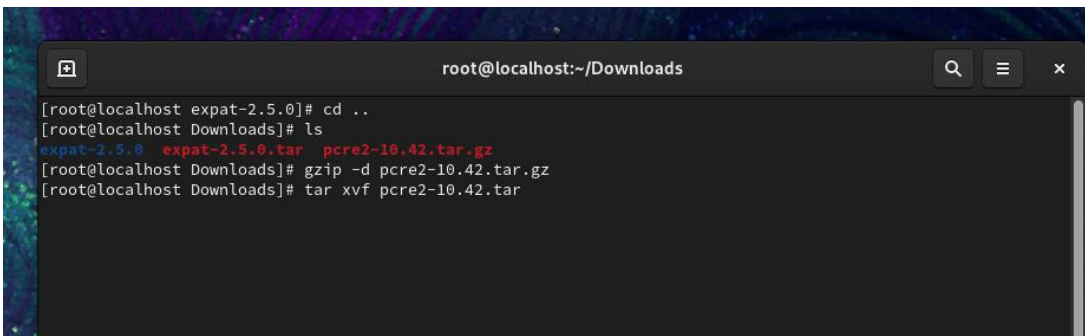


```

root@localhost:~/Downloads
[root@localhost expat-2.5.0]# cd ..
[root@localhost Downloads]# ls
expat-2.5.0  expat-2.5.0.tar  pcre2-10.42.tar.gz
[root@localhost Downloads]# gzip -d pcre2-10.42.tar.gz

```

Imagen 55 Descomprimiendo pcre2. [Fuente Propia]



```

root@localhost:~/Downloads
[root@localhost expat-2.5.0]# cd ..
[root@localhost Downloads]# ls
expat-2.5.0  expat-2.5.0.tar  pcre2-10.42.tar.gz
[root@localhost Downloads]# gzip -d pcre2-10.42.tar.gz
[root@localhost Downloads]# tar xvf pcre2-10.42.tar

```

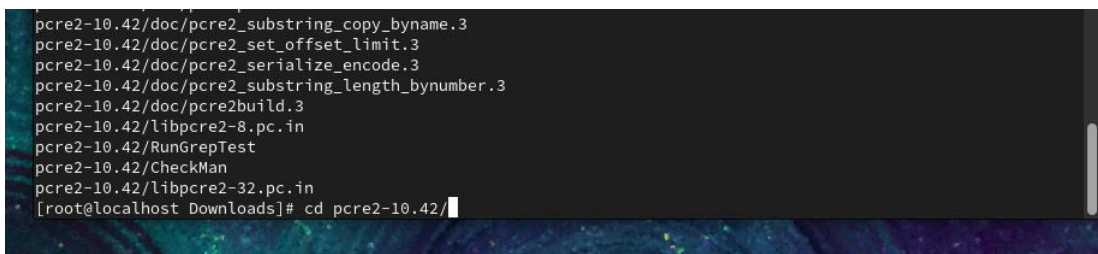
Imagen 56 Descomprimiendo pcre2 imagen 2. [Fuente Propia]

y para instalar, entrar a la carpeta y ejecutar:

```

./configure
make
make install

```

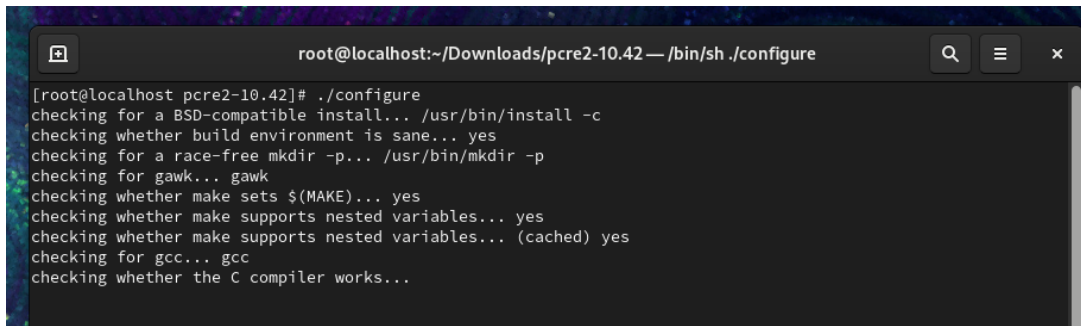


```

pcre2-10.42/doc/pcre2_substring_copy_byname.3
pcre2-10.42/doc/pcre2_set_offset_limit.3
pcre2-10.42/doc/pcre2_serialize_encode.3
pcre2-10.42/doc/pcre2_substring_length_bynumber.3
pcre2-10.42/doc/pcre2build.3
pcre2-10.42/libpcre2-8.pc.in
pcre2-10.42/RunGrepTest
pcre2-10.42/CheckMan
pcre2-10.42/libpcre2-32.pc.in
[root@localhost Downloads]# cd pcre2-10.42/

```

Imagen 57 Ingresando a la carpeta de pcre2. [Fuente Propia]

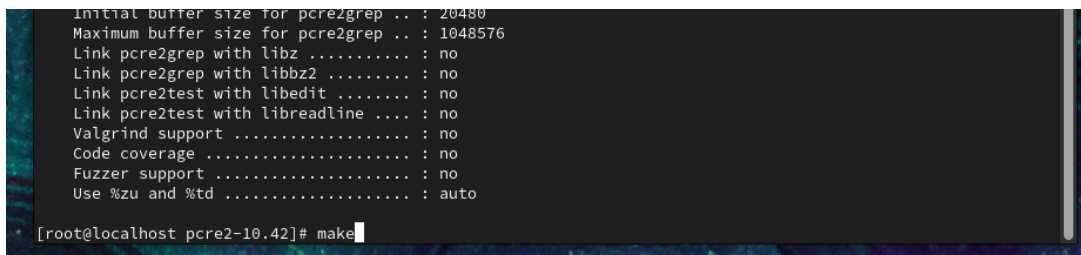


```

root@localhost:~/Downloads/pcr2-10.42 — /bin/sh ./configure
[root@localhost pcre2-10.42]# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a race-free mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports nested variables... (cached) yes
checking for gcc... gcc
checking whether the C compiler works...

```

Imagen 58 Configuración en carpeta de pcre2. [Fuente Propia]



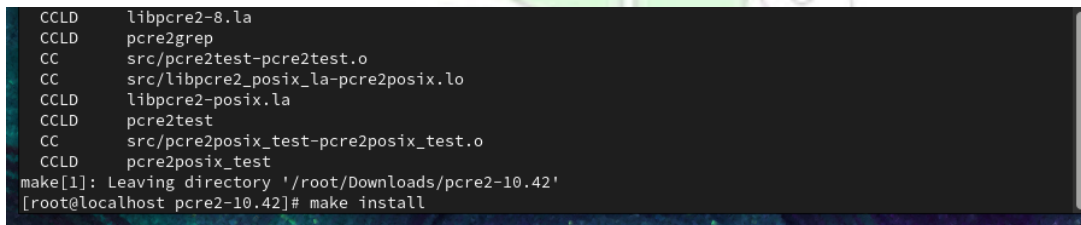
```

Initial buffer size for pcre2grep .. : 20480
Maximum buffer size for pcre2grep .. : 1048576
Link pcre2grep with libz ..... : no
Link pcre2grep with libbz2 ..... : no
Link pcre2test with libedit ..... : no
Link pcre2test with libreadline .... : no
Valgrind support ..... : no
Code coverage ..... : no
Fuzzer support ..... : no
Use %zu and %td ..... : auto

[root@localhost pcre2-10.42]# make

```

Imagen 59 Configuración en carpeta de pcre2 terminada y comienza comando make. [Fuente Propia]

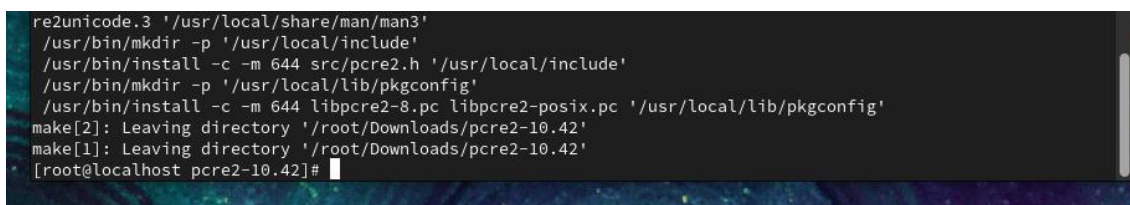


```

CCLD libpcre2-8.la
CCLD pcre2grep
CC src/pcre2test-pcre2test.o
CC src/libpcre2_posix_la-pcre2posix.lo
CCLD libpcre2-posix.la
CCLD pcre2test
CC src/pcre2posix_test-pcre2posix_test.o
CCLD pcre2posix_test
make[1]: Leaving directory '/root/Downloads/pcre2-10.42'
[root@localhost pcre2-10.42]# make install

```

Imagen 60 Comienza comando make install. [Fuente Propia]



```

re2unicode.3 '/usr/local/share/man/man3'
/usr/bin/mkdir -p '/usr/local/include'
/usr/bin/install -c -m 644 src/pcre2.h '/usr/local/include'
/usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
/usr/bin/install -c -m 644 libpcre2-8.pc libpcre2-posix.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/root/Downloads/pcre2-10.42'
make[1]: Leaving directory '/root/Downloads/pcre2-10.42'
[root@localhost pcre2-10.42]#

```

Imagen 61 Comando make install finalizado. [Fuente Propia]

Instalación de APR 1.7.4

Descargar APR desde la página oficial de Apache “apr.apache.org”.

Apache Portable Runtime 1.7.4 Released

The Apache Software Foundation and the Apache Portable Runtime Project are proud to announce the General Availability of version 1.7.4 of the Apache Portable Runtime library. APR 1.7 brings a number of enhancements and bugfixes documented in CHANGES. Users of earlier versions are encouraged to update to this release.

For further details of this release, see the [official announcement](#) as well as the [CHANGES-APR-1.7](#) file.

[Download](#)

Programmer's Manual: [APR](#)

Imagen 62 Página para la descarga de APR 1.7.4. [Fuente apr.apache.org]

Elegir la opción de archivo.tar.gz.

APR 1.7.4 is the best available version

APR is the base portability library.

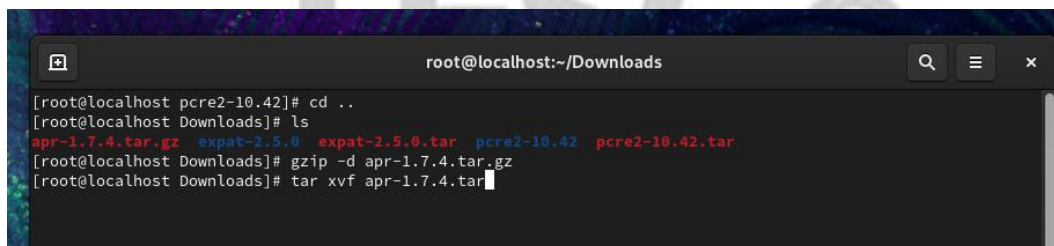
- Unix Source: [apr-1.7.4.tar.gz](#) [PGP] [SHA256]
- Unix Source: [apr-1.7.4.tar.bz2](#) [PGP] [SHA256]
- Win32 Source: [apr-1.7.4-win32-src.zip](#) [PGP] [SHA256]
- [Other files](#)

Imagen 63 Sección para la descarga de APR 1.7.4. [Fuente apr.apache.org]

Ejecutar los comandos para descomprimir:

`gzip -d archivo.tar.gz`

`tar xvf archivo.tar`



```
root@localhost:~/Downloads
[root@localhost pcre2-10.42]# cd ..
[root@localhost Downloads]# ls
apr-1.7.4.tar.gz  expat-2.5.0  expat-2.5.0.tar  pcre2-10.42  pcre2-10.42.tar
[root@localhost Downloads]# gzip -d apr-1.7.4.tar.gz
[root@localhost Downloads]# tar xvf apr-1.7.4.tar
```

Imagen 64 Descomprimir apr 1.7.4. [Fuente Propia]

y para instalar, entrar a la carpeta y ejecutar:

`./configure`

`make`

make install

```
apr-1.7.4/misc/unix/charset.c
apr-1.7.4/misc/unix/getopt.c
apr-1.7.4/misc/unix/start.c
apr-1.7.4/misc/netware/rand.c
apr-1.7.4/misc/netware/apr.xdc
apr-1.7.4/misc/netware/aprlib.def
apr-1.7.4/misc/netware/charset.c
apr-1.7.4/misc/netware/start.c
apr-1.7.4/misc/netware/libprews.c
[root@localhost Downloads]# cd apr-1.7.4/
[root@localhost apr-1.7.4]# ./configure
```

Imagen 65 Comando configure en apr 1.7.4. [Fuente Propia]

```
config.status: creating build/pkg/pkginfo
config.status: creating apr-1-config
config.status: creating apr.pc
config.status: creating test/Makefile
config.status: creating test/internal/Makefile
config.status: creating include/arch/unix/apr_private.h
config.status: executing libtool commands
rm: cannot remove 'libtool': No such file or directory
config.status: executing default commands
[root@localhost apr-1.7.4]# make
```

Imagen 66 Comando make en apr 1.7.4. [Fuente Propia]

```
arch/unix -I./include/arch/unix -I/root/Downloads/apr-1.7.4/include/arch/unix -I/root/Downloads/apr-1.7.4/inc
lude -I/root/Downloads/apr-1.7.4/include/private -I/root/Downloads/apr-1.7.4/include/private exports.c | gre
p "ap_hack_" | sed -e 's/^(.*)\((.*)\);$/\1/' >> apr.exp
gcc -E -DHAVE_CONFIG_H -DLINUX -D_REENTRANT -D_GNU_SOURCE -I./include -I/root/Downloads/apr-1.7.4/include/
arch/unix -I./include/arch/unix -I/root/Downloads/apr-1.7.4/include/arch/unix -I/root/Downloads/apr-1.7.4/inc
lude -I/root/Downloads/apr-1.7.4/include/private -I/root/Downloads/apr-1.7.4/include/private export_vars.c |
sed -e 's/^\#[^!]*// ' | sed -e '/^$/d' >> apr.exp
sed 's,^\(location=\).*$,\\installed,' < apr-1-config > apr-config.out
sed -e 's,^\(apr_build.*=\).*$,\\usr/local/apr/build-1,' -e 's,^\(top_build.*=\).*$,\\usr/local/apr/build-1
,' < build/apr_rules.mk > build/apr_rules.out
make[1]: Leaving directory '/root/Downloads/apr-1.7.4'
[root@localhost apr-1.7.4]# make install
```

Imagen 67 Comando make install en apr 1.7.4. [Fuente Propia]

```
/usr/bin/install -c -m 755 /root/Downloads/apr-1.7.4/build/mkdir.sh /usr/local/apr/build-1
for f in make_exports.awk make_var_export.awk; do \
    /usr/bin/install -c -m 644 /root/Downloads/apr-1.7.4/build/${f} /usr/local/apr/build-1; \
done
/usr/bin/install -c -m 644 build/apr_rules.out /usr/local/apr/build-1/apr_rules.mk
/usr/bin/install -c -m 755 apr-config.out /usr/local/apr/bin/apr-1-config
[root@localhost apr-1.7.4]#
```

Imagen 68 Comando make install finalizado en apr 1.7.4. [Fuente Propia]

Instalación de APR-Util 1.6.3

Descargar APR-Util desde la página oficial de Apache “apr.apache.org”.

Apache Portable Runtime Utility 1.6.3 Released

The Apache Software Foundation and the Apache Portable Runtime Project are proud to announce the General Availability of version 1.6.3 of the APR Apache Portable Runtime Utility library. Users of earlier versions are encouraged to update to this release.

The main changes in this release are concerned with the third-party dependencies, including unbundling expat, and building with up-to-date versions of libraries such as OpenSSL and MySQL.

For further details of this release, see the [official announcement](#) as well as the [CHANGES-APR-UTIL-1.6](#) file.

[Download](#)

Programmer's Manual: [APR-util](#)

Imagen 69 Página para la descarga de APR Util 1.6.3. [Fuente apr.apache.org]

Elegir la opción de archivo.tar.gz.

APR-util 1.6.3 is the best available version

APR-util provides a number of helpful abstractions on top of APR.

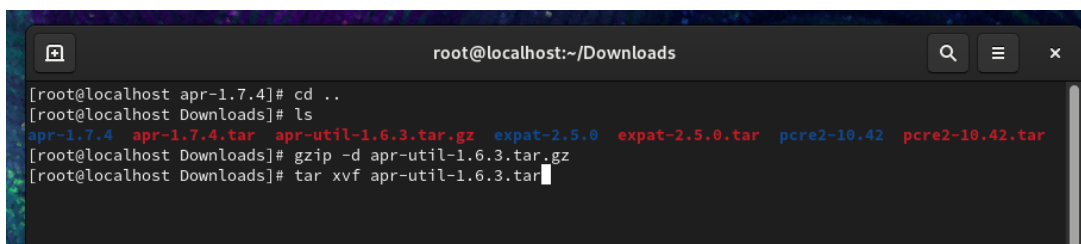
- Unix Source: [apr-util-1.6.3.tar.gz](#) [PGP] [SHA256]
- Unix Source: [apr-util-1.6.3.tar.bz2](#) [PGP] [SHA256]
- Windows Source: [apr-util-1.6.3-win32-src.zip](#) [PGP] [SHA256]
- [Other files](#)

Imagen 70 Sección para la descarga de APR Util 1.6.3. [Fuente apr.apache.org]

Ejecutar los comandos para descomprimir:

`gzip -d archivo.tar.gz`

`tar xvf archivo.tar`



```

root@localhost:~/Downloads
[root@localhost apr-1.7.4]# cd ..
[root@localhost Downloads]# ls
apr-1.7.4  apr-1.7.4.tar  apr-util-1.6.3.tar.gz  expat-2.5.0  expat-2.5.0.tar  pcre2-10.42  pcre2-10.42.tar
[root@localhost Downloads]# gzip -d apr-util-1.6.3.tar.gz
[root@localhost Downloads]# tar xvf apr-util-1.6.3.tar

```

Imagen 71 Descomprimiendo APR Util 1.6.3. [Fuente Propia]

```
apr-util-1.6.3/buckets/apr_buckets_refcount.c
apr-util-1.6.3/buckets/apr_buckets_alloc.c
apr-util-1.6.3/buckets/apr_buckets_eos.c
apr-util-1.6.3/buckets/apr_buckets.c
apr-util-1.6.3/buckets/apr_buckets_socket.c
apr-util-1.6.3/buckets/apr_buckets_flush.c
apr-util-1.6.3/buckets/apr_buckets_pool.c
[root@localhost Downloads]#
```

Imagen 72 Descomprimiendo APR Util 1.6.3 imagen 2. [Fuente Propia]

y para instalar, entrar a la carpeta y ejecutar:

```
./configure --with-apr=/usr/local/apr/bin/apr-1-config
make
make install
```

--with-apr es la dirección de un archivo de configuración de APR que necesita APR-Util. Al intentar ejecutar únicamente “./configure” en APR-Util, al finalizar mostrara un error en la terminar acompañado de la solución la cual debe de indicarse la dirección “/usr/local/apr/bin/apr-1-config”.

```
root@localhost:~/Downloads/apr-util-1.6.3
[root@localhost Downloads]# cd apr-util-1.6.3/
[root@localhost apr-util-1.6.3]# ./configure --with-apr=/usr/local/apr/bin/apr-1-config
configure: error: invalid variable name: `--with-apr'
[root@localhost apr-util-1.6.3]# ./configure --with-apr=/usr/local/apr/bin/apr-1-config
```

Imagen 73 Comando configure en APR Util 1.6.3. [Fuente Propia]

```
config.status: creating include/apr_ldap.h
config.status: creating include/apu.h
config.status: creating include/apu_want.h
config.status: creating test/Makefile
config.status: creating include/private/apu_config.h
config.status: executing default commands
[root@localhost apr-util-1.6.3]# make
```

Imagen 74 Comando make en APR Util 1.6.3. [Fuente Propia]

```
vate/apr_dbm_private.h /root/Downloads/apr-util-1.6.3/include/private/apu_internal.h > export_vars.c
gcc -E -DHAVE_CONFIG_H -DLINUX -D_REENTRANT -D_GNU_SOURCE -I/root/Downloads/apr-util-1.6.3/include -I/root
/Downloads/apr-util-1.6.3/include/private -I/usr/local/apr/include/apr-1 exports.c | grep "ap_hack_" | se
d -e 's/^.*[)](.*);$/\1/' >> aprutil.exp
gcc -E -DHAVE_CONFIG_H -DLINUX -D_REENTRANT -D_GNU_SOURCE -I/root/Downloads/apr-util-1.6.3/include -I/root
/Downloads/apr-util-1.6.3/include/private -I/usr/local/apr/include/apr-1 export_vars.c | sed -e 's/^\#[^!
]*// ' | sed -e '/^$/d' >> aprutil.exp
sed 's,^\(location=\).*$,\\installed,' < apu-1-config > apu-config.out
make[1]: Leaving directory '/root/Downloads/apr-util-1.6.3'
[root@localhost apr-util-1.6.3]# make install
```

Imagen 75 Comando make install en APR Util 1.6.3. [Fuente Propia]

```
- use the -Wl, -rpath -Wl,LIBDIR linker flag
- have your system administrator add LIBDIR to '/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
-----
/usr/bin/install -c -m 644 aprutil.exp /usr/local/apr/lib
/usr/bin/install -c -m 755 apu-config.out /usr/local/apr/bin/apu-1-config
[root@localhost apr-util-1.6.3]#
```

Imagen 76 Comando make install finalizado en APR Util 1.6.3. [Fuente Propia]

Instalación de Apache Server

En Apache y la página web de PHP se encuentran 3 maneras de instalar Apache

Tabla 48 Maneras de instalar PHP. [Fuente Propia]

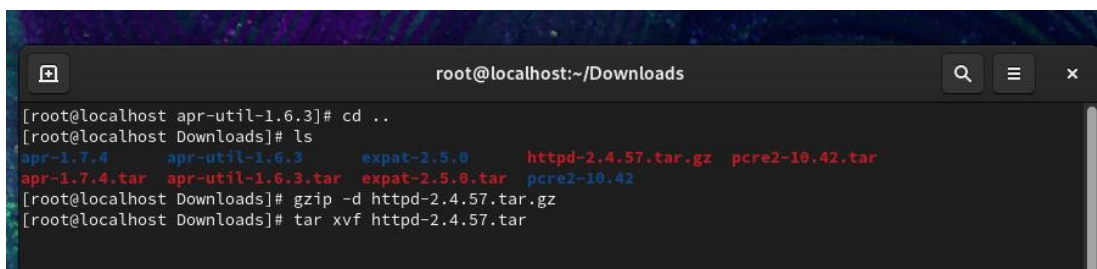
Web Site	Comando
Apache.org	sudo yum install httpd
Apache.org	Download the latest release from http://httpd.apache.org/download.cgi Extract \$ gzip -d httpd-NN.tar.gz \$ tar xvf httpd-NN.tar \$ cd httpd-NN Configure \$./configure --prefix=PREFIX Compile \$ make Install \$ make install Customize \$ vi PREFIX/conf/httpd.conf Test \$ PREFIX/bin/apachectl -k start PREFIX es comúnmente /usr/local/apache2
PHP	tar -xzf httpd-2.x.NN.tar.gz cd httpd-2_x_NN ./configure --enable-so make make install

La opción recomendada es desde la página oficial de Apache e instalando desde el archivo.tar.gz descargable de “httpd.apache.org/download.cgi#apache24”.

Ejecutar los comandos para descomprimir:

`gzip -d archivo.tar.gz`

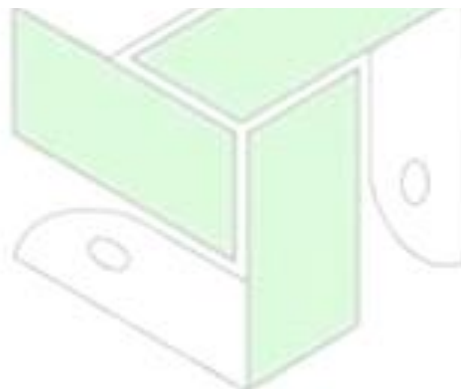
`tar xvf archivo.tar`



```

root@localhost:~/Downloads
[root@localhost apr-util-1.6.3]# cd ..
[root@localhost Downloads]# ls
apr-1.7.4      apr-util-1.6.3      expat-2.5.0      httpd-2.4.57.tar.gz  pcre2-10.42.tar
apr-1.7.4.tar  apr-util-1.6.3.tar  expat-2.5.0.tar  pcre2-10.42
[root@localhost Downloads]# gzip -d httpd-2.4.57.tar.gz
[root@localhost Downloads]# tar xvf httpd-2.4.57.tar
    
```

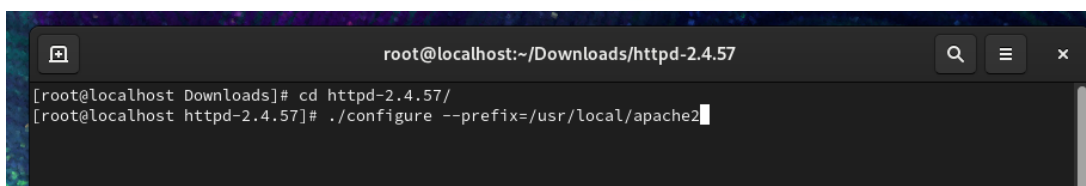
Imagen 77 Descomprimiendo httpd. [Fuente Propia]



Ingresa y configura:

`cd httpd-NN`

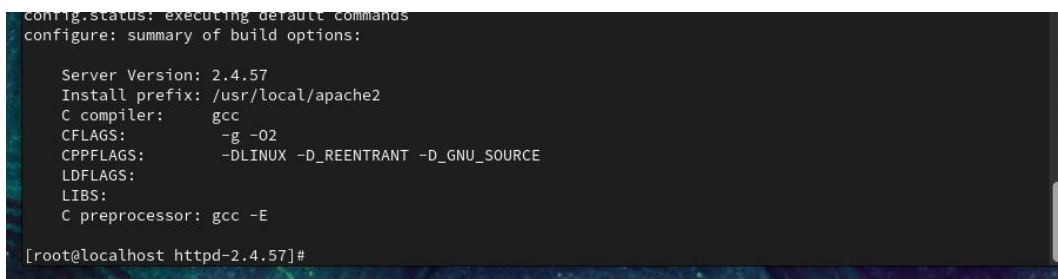
`./configure --prefix=PREFIX`



```

root@localhost:~/Downloads/httpd-2.4.57
[root@localhost Downloads]# cd httpd-2.4.57/
[root@localhost httpd-2.4.57]# ./configure --prefix=/usr/local/apache2
    
```

Imagen 78 Comando configure en httpd. [Fuente Propia]



```

config.status: executing default commands
configure: summary of build options:

  Server Version: 2.4.57
  Install prefix: /usr/local/apache2
  C compiler:      gcc
  CFLAGS:          -g -O2
  CPPFLAGS:        -DLINUX -D_REENTRANT -D_GNU_SOURCE
  LDFLAGS:
  LIBS:
  C preprocessor:  gcc -E

[root@localhost httpd-2.4.57]#
    
```

Imagen 79 Comando configure finalizado en httpd. [Fuente Propia]

Instalar y compilar:

Make

Make install

```
/apache2/modules -module -avoid-version mod_rewrite.lo
make[4]: Leaving directory '/root/Downloads/httpd-2.4.57/modules/mappers'
make[3]: Leaving directory '/root/Downloads/httpd-2.4.57/modules/mappers'
make[2]: Leaving directory '/root/Downloads/httpd-2.4.57/modules'
make[2]: Entering directory '/root/Downloads/httpd-2.4.57/support'
make[2]: Leaving directory '/root/Downloads/httpd-2.4.57/support'

make[1]: Leaving directory '/root/Downloads/httpd-2.4.57'
[root@localhost httpd-2.4.57]# make
```

Imagen 80 Comando make en httpd. [Fuente Propia]

```
make[3]: Leaving directory '/root/Downloads/httpd-2.4.57/modules/mappers'
make[2]: Leaving directory '/root/Downloads/httpd-2.4.57/modules'
make[2]: Entering directory '/root/Downloads/httpd-2.4.57/support'
make[2]: Leaving directory '/root/Downloads/httpd-2.4.57/support'

make[1]: Leaving directory '/root/Downloads/httpd-2.4.57'
[root@localhost httpd-2.4.57]# make install
```

Imagen 81 Comando make install en httpd. [Fuente Propia]

Instalación de MySQL

Descargar e instalar el Mysql community reléase. Este es un repositorio de mysql, quiere decir que contendrá archivos que serán necesarios para el funcionamiento de mysql server. Descargar de “dev.mysql.com/downloads/repo/yum/” el archivo para Red Hat Enterprise Linux 9.

MySQL Community Downloads

MySQL Yum Repository

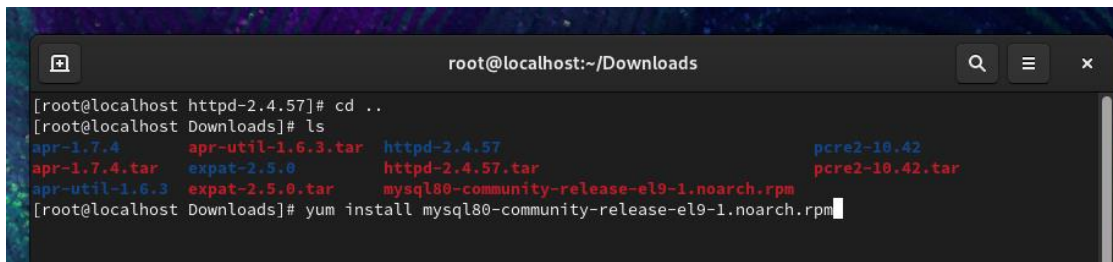
Repository Setup Packages

Red Hat Enterprise Linux 9 / Oracle Linux 9 (Architecture Independent), RPM Package (mysql80-community-release-el9-1.noarch.rpm)	10.3K	Download
MD5: d07a0c6a95783c43d0c520c245cf18e0		

Imagen 82 Descarga de MySQL Community oficial. [Fuente dev.mysql.com/downloads/repo/yum/]

Ejecutar los comandos para instalar:

\$> sudo yum install mysql80-community-release-el9-{version-number}.noarch.rpm



```

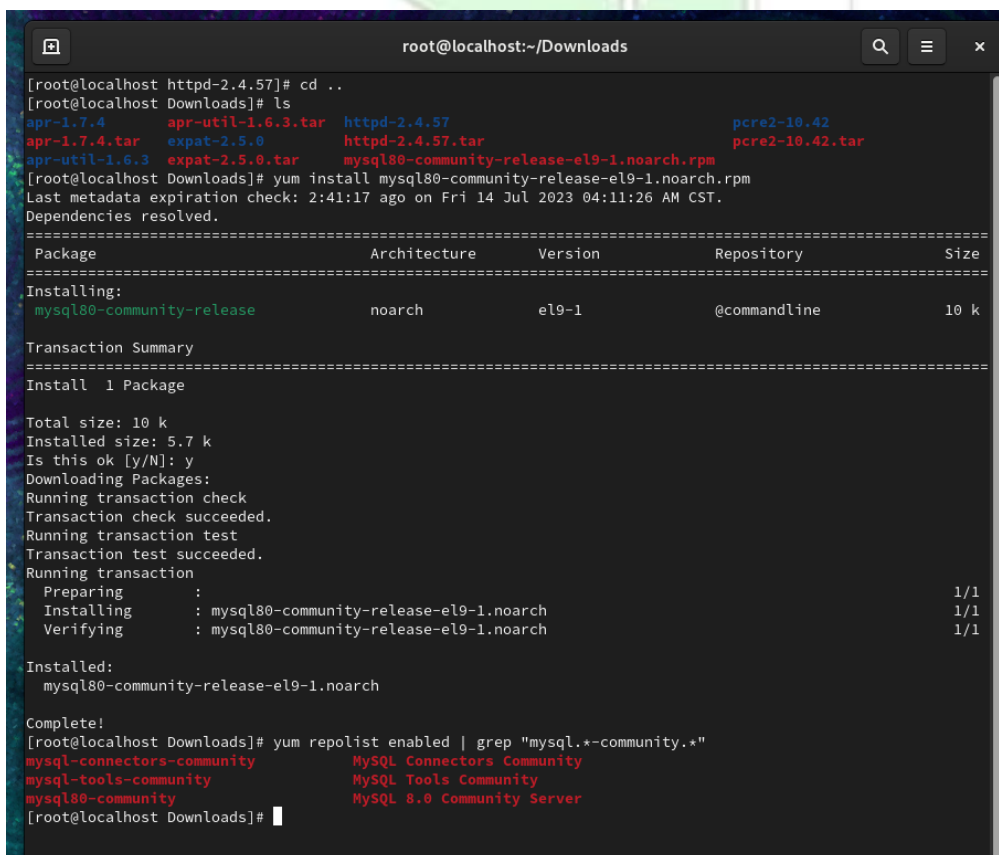
root@localhost:~/Downloads
[root@localhost httpd-2.4.57]# cd ..
[root@localhost Downloads]# ls
apr-1.7.4      apr-util-1.6.3.tar  httpd-2.4.57      pcre2-10.42
apr-1.7.4.tar  expat-2.5.0        httpd-2.4.57.tar  pcre2-10.42.tar
apr-util-1.6.3  expat-2.5.0.tar    mysql80-community-release-el9-1.noarch.rpm
[root@localhost Downloads]# yum install mysql80-community-release-el9-1.noarch.rpm

```

Imagen 83 Instalación de MySQL Community oficial. [Fuente Propia]

El siguiente comando habilita y muestra que el repositorio de MySQL se haya añadido:

\$> yum repolist enabled | grep "mysql.*-community.*"



```

root@localhost:~/Downloads
[root@localhost httpd-2.4.57]# cd ..
[root@localhost Downloads]# ls
apr-1.7.4      apr-util-1.6.3.tar  httpd-2.4.57      pcre2-10.42
apr-1.7.4.tar  expat-2.5.0        httpd-2.4.57.tar  pcre2-10.42.tar
apr-util-1.6.3  expat-2.5.0.tar    mysql80-community-release-el9-1.noarch.rpm
[root@localhost Downloads]# yum install mysql80-community-release-el9-1.noarch.rpm
Last metadata expiration check: 2:41:17 ago on Fri 14 Jul 2023 04:11:26 AM CST.
Dependencies resolved.
=====
Package                                Architecture Version      Repository    Size
=====
Installing:
mysql80-community-release              noarch      el9-1        @commandline  10 k
Transaction Summary
=====
Install 1 Package
Total size: 10 k
Installed size: 5.7 k
Is this ok [y/N]: y
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : mysql80-community-release-el9-1.noarch 1/1
  Verifying      : mysql80-community-release-el9-1.noarch 1/1

Installed:
mysql80-community-release-el9-1.noarch

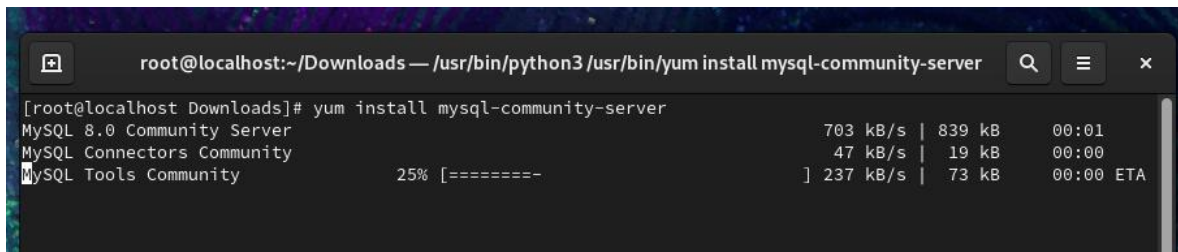
Complete!
[root@localhost Downloads]# yum repolist enabled | grep "mysql.*-community.*"
mysql-connectors-community      MySQL Connectors Community
mysql-tools-community          MySQL Tools Community
mysql80-community              MySQL 8.0 Community Server
[root@localhost Downloads]#

```

Imagen 84 Muestra de la instalación del repositorio MySQL Community oficial. [Fuente Propia]

Instalar MySQL por medio del siguiente comando:

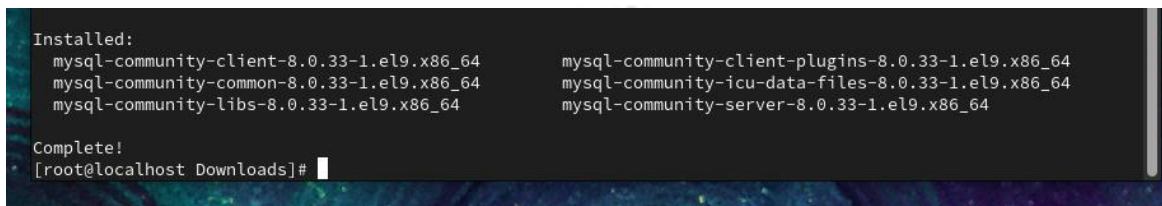
\$> sudo yum install mysql-community-server



```

root@localhost:~/Downloads — /usr/bin/python3 /usr/bin/yum install mysql-community-server
[root@localhost Downloads]# yum install mysql-community-server
MySQL 8.0 Community Server              703 kB/s | 839 kB      00:01
MySQL Connectors Community             47 kB/s | 19 kB       00:00
MySQL Tools Community                  25% [=====
] 237 kB/s | 73 kB     00:00 ETA
  
```

Imagen 85 Instalación de MySQL Community server. [Fuente Propia]



```

Installed:
mysql-community-client-8.0.33-1.el9.x86_64    mysql-community-client-plugins-8.0.33-1.el9.x86_64
mysql-community-common-8.0.33-1.el9.x86_64    mysql-community-icu-data-files-8.0.33-1.el9.x86_64
mysql-community-libs-8.0.33-1.el9.x86_64      mysql-community-server-8.0.33-1.el9.x86_64

Complete!
[root@localhost Downloads]#
  
```

Imagen 86 Instalación completa de MySQL Community server. [Fuente Propia]

Inicia el servidor con el siguiente comando:

\$> systemctl start mysqld

El usuario root de MySQL tendrá una contraseña temporal, la cual debe cambiarse una vez ingresa al servidor.

Primero ingresar el siguiente código para obtener la contraseña:

\$> sudo grep 'temporary password' /var/log/mysqld.log

Ingresa al servidor de mysql:

\$> mysql -uroot -p

```
[root@localhost Downloads]# systemctl start mysqld
[root@localhost Downloads]# grep 'temporary password' /var/log/mysqld.log
2023-07-14T13:24:57.111482Z 6 [Note] [MY-010454] [Server] A temporary password is generated for root@localhost: gLS.7J8fId-
[root@localhost Downloads]# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.33

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Imagen 87 Ingreso al servidor de MySQL server. [Fuente Propia]

Cambia la contraseña colocando la nueva en lugar de MyNewPass4!:

mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY 'MyNewPass4!';

```
mysql> ALTER USER 'root'@'localhost' IDENTIFIED BY '#MyNewPass4RootDB';
Query OK, 0 rows affected (0.04 sec)

mysql>
```

Imagen 88 Cambio de contraseña de MySQL server. [Fuente Propia]

Instalación de PHP

Descargar de [php.net/releases/](https://www.php.net/releases/) la versión deseada, en este caso basado en los requerimientos de Zabbix Server V6.0 la versión de PHP debe ser V7.2.5 o superior e inferior a 8.0. La opción elegida es la Versión V7.3.33

Descomprime y ejecuta para instalar:

```
root@localhost:~/Downloads
[root@localhost Downloads]# ls
apr-1.7.4      apr-util-1.6.3.tar  httpd-2.4.57      pcre2-10.42
apr-1.7.4.tar  expat-2.5.0        httpd-2.4.57.tar  pcre2-10.42.tar
apr-util-1.6.3  expat-2.5.0.tar    mysql80-community-release-el9-1.noarch.rpm  php-7.3.33.tar.gz
[root@localhost Downloads]# gzip -d php-7.3.33.tar.gz
[root@localhost Downloads]# tar xvf php-7.3.33.tar
```

Imagen 89 Descomprimiendo php 7.3.33. [Fuente Propia]

```
cd ../php-NN
```

```
./configure --with-apxs2=/usr/local/apache2/bin/apxs --with-pdo-mysql
```

```
make
```

```
make install
```

```
php-7.3.33/Zend/Zend/zend_vm_trace_handlers.h
php-7.3.33/Zend/Zend/zend_objects_API.h
php-7.3.33/Zend/Zend/zend_ini_parser.output
php-7.3.33/Zend/Zend/zend_ini_scanner.c
php-7.3.33/Zend/Zend/zend_float.h
php-7.3.33/Zend/Zend/zend_alloc.h
php-7.3.33/Zend/Zend/zend_alloc.m4
php-7.3.33/makedist
[root@localhost Downloads]# cd php-7.3.33/
[root@localhost php-7.3.33]# ./configure --with-apxs2=/usr/local/apache2/bin/apxs --with-pdo-mysql
```

Imagen 90 Comando configure en php 7.3.33. [Fuente Propia]

```
config.status: creating sapi/phpdbg/phpdbg.1
config.status: creating sapi/cgi/php-cgi.1
config.status: creating ext/phar/phar.1
config.status: creating ext/phar/phar.phar.1
config.status: creating main/php_config.h
config.status: executing default commands
[root@localhost php-7.3.33]#
```

Imagen 91 Comando configure finalizado en php 7.3.33. [Fuente Propia]

```
config.status: creating main/php_config.h
config.status: executing default commands
[root@localhost php-7.3.33]# make
/bin/sh /root/Downloads/php-7.3.33/libtool --silent --preserve-dup-deps --mode=compile cc -Iext/date/lib -DZEN
ND_ENABLE_STATIC_TSRMLS_CACHE=1 -DHAVE_TIMELIB_CONFIG_H=1 -Iext/date/ -I/root/Downloads/php-7.3.33/ext/date/
-DPHP_ATOM_INC -I/root/Downloads/php-7.3.33/include -I/root/Downloads/php-7.3.33/main -I/root/Downloads/php-7
.3.33 -I/root/Downloads/php-7.3.33/ext/date/lib -I/usr/include/libxml2 -I/root/Downloads/php-7.3.33/ext/sqlit
e3/libsqlite -I/root/Downloads/php-7.3.33/TSRM -I/root/Downloads/php-7.3.33/Zend -D_REENTRANT -pthread -I/u
sr/include -g -O2 -fvisibility=hidden -pthread -DZTS -DZEND_SIGNALS -c /root/Downloads/php-7.3.33/ext/date/
php_date.c -o ext/date/php_date.lo
```

Imagen 92 Comando make en php 7.3.33. [Fuente Propia]

```

Generating phar.phar
PEAR package PHP_Archive not installed: generated phar will require PHP's phar extension be enabled.
clicommand.inc
directorytreeiterator.inc
pharcommand.inc
directorygraphiterator.inc
invertedregexiterator.inc
phar.inc

Build complete.
Don't forget to run 'make test'.

[root@localhost php-7.3.33]# make install

```

Imagen 93 Comando make install en php 7.3.33

```

[PEAR] PEAR - installed: 1.10.13
Wrote PEAR system config file at: /usr/local/etc/pear.conf
You may want to add: /usr/local/lib/php to your php.ini include_path
/root/Downloads/php-7.3.33/build/shtool install -c ext/phar/phar.phar /usr/local/bin
ln -s -f phar.phar /usr/local/bin/phar
Installing PDO headers: /usr/local/include/php/ext/pdo/
[root@localhost php-7.3.33]#

```

Imagen 94 Comando make install finalizado en php 7.3.33. [Fuente Propia]

Nota: En caso de mostrar la terminal un error sobre la librería libxml2-deve faltante, se puede instalar con el comando: `yum install libxml2-devel`

```

Checking whether to enable LibXML support... yes
checking libxml2 install dir... no
checking for xml2-config path...
checking for pkg-config... /usr/bin/pkg-config
configure: error: libxml2 not found. Please check your libxml2 installation.
[root@localhost php-7.3.33]# yum install libxml2-devel
Last metadata expiration check: 2:13:23 ago on Sat 15 Jul 2023 05:35:26 AM CST.
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
libxml2-devel           x86_64            2.9.13-4.el9     appstream         899 k
Installing dependencies:
cmake-filesystem        x86_64            3.20.2-8.el9     appstream         19 k
Transaction Summary
=====
Install 2 Packages

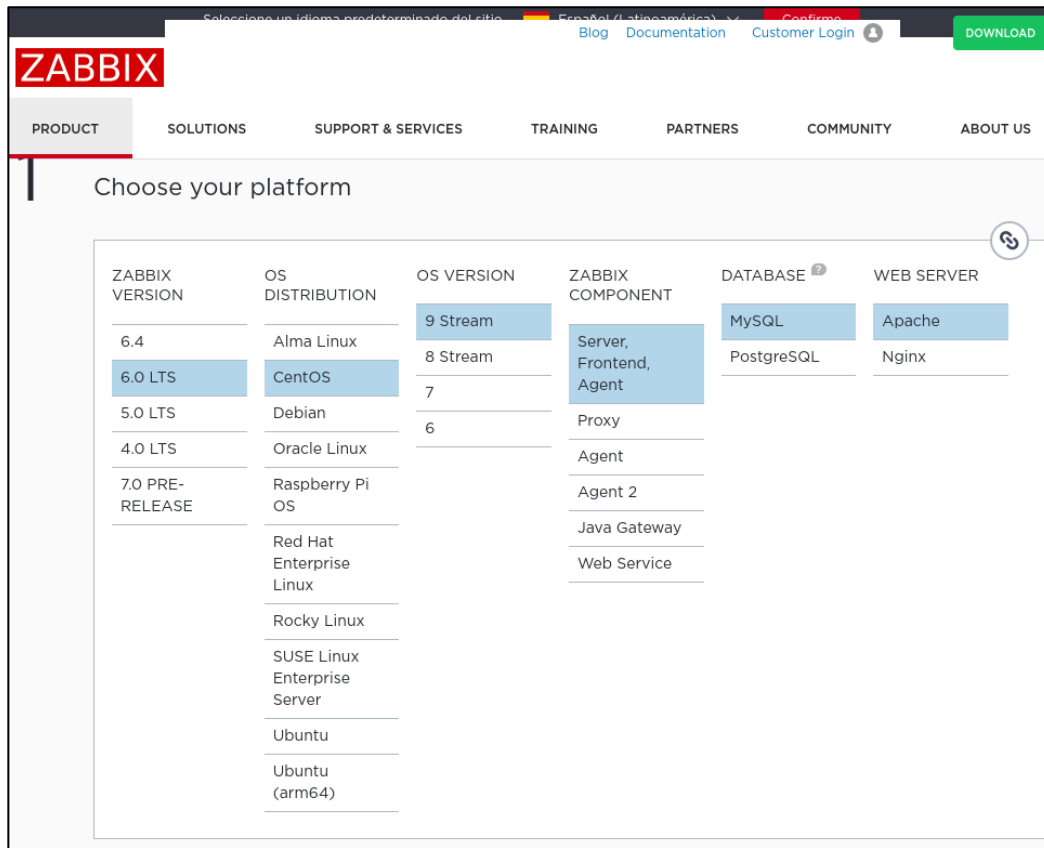
Total download size: 917 k
Installed size: 8.8 M
Is this ok [y/N]:

```

Imagen 95 Error e instalación de librería libxml2 para php 7.3.33. [Fuente Propia]

Instalación y configuración de Zabbix Server

Escoger la versión a instalar de Zabbix. S.O., componentes, base de datos y web server. Se ha elegido la versión V6.0, es una versión anterior a la más actual, la documentación de la instalación de Zabbix se encuentra en su página oficial, en el ítem del menú principal “PRODUCT - Download and install Zabbix”.



The screenshot shows the Zabbix website's download page. At the top, there's a navigation bar with links for Blog, Documentation, Customer Login, and a DOWNLOAD button. Below this is a main navigation bar with links for PRODUCT, SOLUTIONS, SUPPORT & SERVICES, TRAINING, PARTNERS, COMMUNITY, and ABOUT US. The main content area is titled 'Choose your platform' and contains a form with several columns of options:

ZABBIX VERSION	OS DISTRIBUTION	OS VERSION	ZABBIX COMPONENT	DATABASE	WEB SERVER	
6.4	Alma Linux	9 Stream	Server, Frontend, Agent	MySQL	Apache	
6.0 LTS	CentOS	8 Stream		PostgreSQL	Nginx	
5.0 LTS	Debian	7		Proxy		
4.0 LTS	Oracle Linux	6		Agent		
7.0 PRE-RELEASE	Raspberry Pi OS			Agent 2		
	Red Hat Enterprise Linux		Java Gateway			
	Rocky Linux		Web Service			
	SUSE Linux Enterprise Server					
	Ubuntu					
	Ubuntu (arm64)					

Imagen 96 Selección de versión de Zabbix para descargar. [Fuente zabbix.com/download]

Instalar el repositorio de Zabbix:

```
# rpm -Uvh https://repo.zabbix.com/zabbix/6.0/rhel/9/x86_64/zabbix-release-6.0-4.el9.noarch.rpm
```

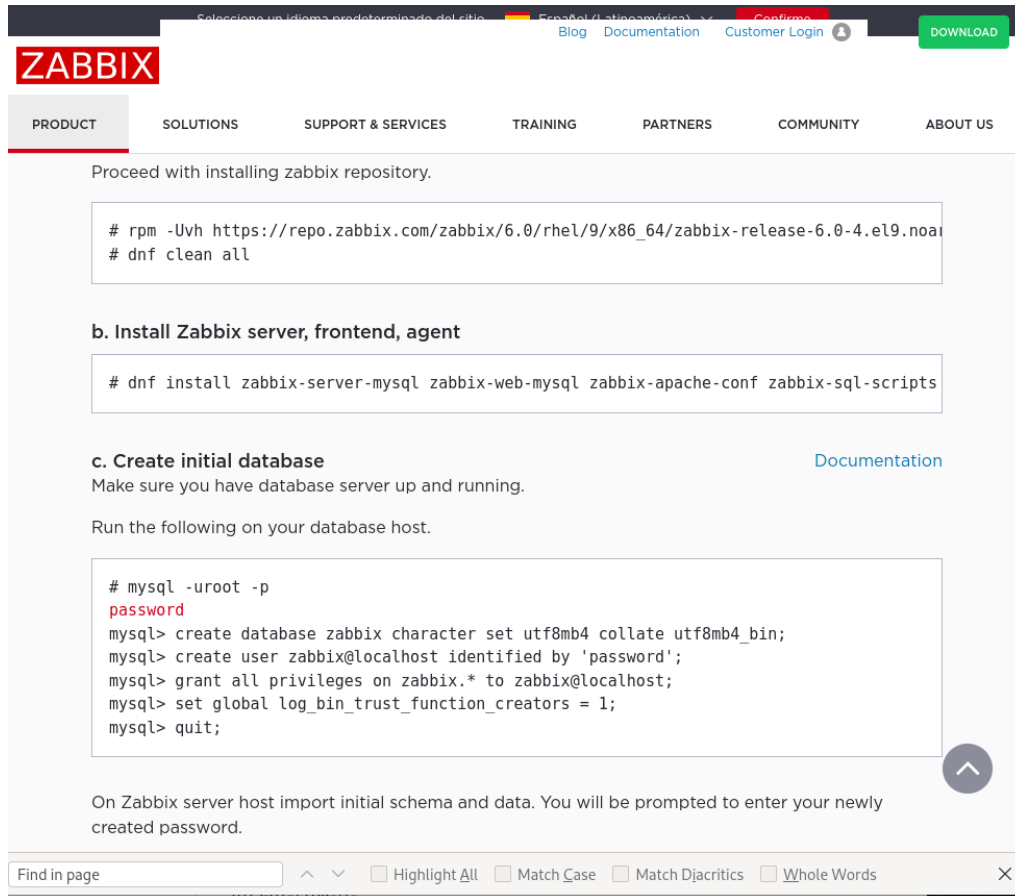


Imagen 97 Instalación del repositorio de zabbix. [Fuente zabbix.com/download]

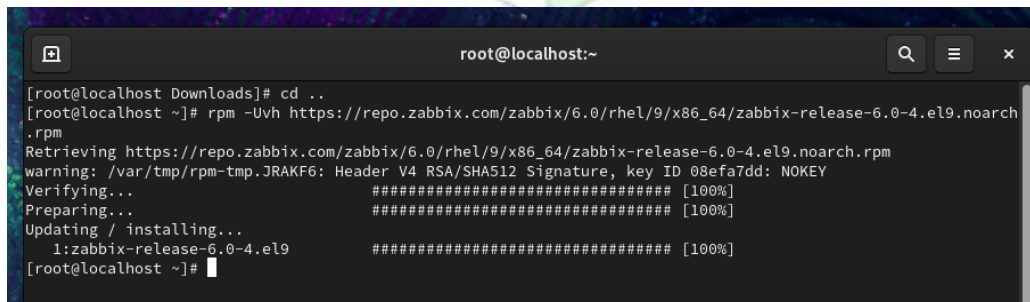


Imagen 98 Instalación del repositorio de zabbix en consola. [Fuente Propia]

Instalar Zabbix server, frontend y agente

```
# dnf clean all
```

```
# dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts
zabbix-selinux-policy zabbix-agent
```

```

root@localhost:~
[root@localhost Downloads]# cd ..
[root@localhost ~]# rpm -Uvh https://repo.zabbix.com/zabbix/6.0/rhel/9/x86_64/zabbix-release-6.0-4.el9.noarch.rpm
Retrieving https://repo.zabbix.com/zabbix/6.0/rhel/9/x86_64/zabbix-release-6.0-4.el9.noarch.rpm
warning: /var/tmp/rpm-tmp.JRAKF6: Header V4 RSA/SHA512 Signature, key ID 08efa7dd: NOKEY
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
 1:zabbix-release-6.0-4.el9 ##### [100%]
[root@localhost ~]# dnf clean all
36 files removed
[root@localhost ~]# dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent

```

Imagen 99 Instalación de zabbix server frontend de zabbix en consola. [Fuente Propia]

Crear una base de datos para Zabbix en MySQL

mysql -uroot -p

password

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;

```

zabbix-agent-6.0.19-release1.el9.x86_64      zabbix-apache-conf-6.0.19-release1.el9.noarch
zabbix-selinux-policy-6.0.19-release1.el9.x86_64  zabbix-server-mysql-6.0.19-release1.el9.x86_64
zabbix-sql-scripts-6.0.19-release1.el9.noarch    zabbix-web-6.0.19-release1.el9.noarch
zabbix-web-deps-6.0.19-release1.el9.noarch       zabbix-web-mysql-6.0.19-release1.el9.noarch

Complete!
[root@localhost ~]# mysql -uroot -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
[root@localhost ~]# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.33 MySQL Community Server - GPL

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;

```

Imagen 100 Creación de base de datos para zabbix en mysql. [Fuente Propia]

mysql> create user zabbix@localhost identified by 'password';

mysql> grant all privileges on zabbix.* to zabbix@localhost;

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.01 sec)

mysql> create user zabbix@localhost identified by '[REDACTED]';
Query OK, 0 rows affected (0.05 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.01 sec)

mysql>
```

Imagen 101 Creación de usuario y asignar todos los privilegios para zabbix en mysql. [Fuente Propia]

```
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

```
mysql> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0.00 sec)

mysql> quit
Bye
[root@localhost ~]#
```

Imagen 102 Set log_bin_trust_function_creators = 1. [Fuente Propia]

Importar al host del servidor de zabbix el esquema y los datos

```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-
set=utf8mb4 -uzabbix -p zabbix
```

```
root@localhost:~
[root@localhost ~]# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Enter password:
[root@localhost ~]#
```

Imagen 103 Importando el host de zabbix. [Fuente Propia]

Deshabilitar log_bin_trust_function_creators

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
```

mysql> quit;

```
[root@localhost ~]# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.33 MySQL Community Server - GPL

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> set global log_bin_trust_function_creators = 0;
Query OK, 0 rows affected (0.00 sec)

mysql> quit
Bye
[root@localhost ~]#
```

Imagen 104 Deshabilitar log_bin_trust_function_creators. [Fuente Propia]

Configurar la base de datos para Zabbix Server entrando a la siguiente dirección y editando el archivo: /etc/zabbix/zabbix_server.conf



TESCO

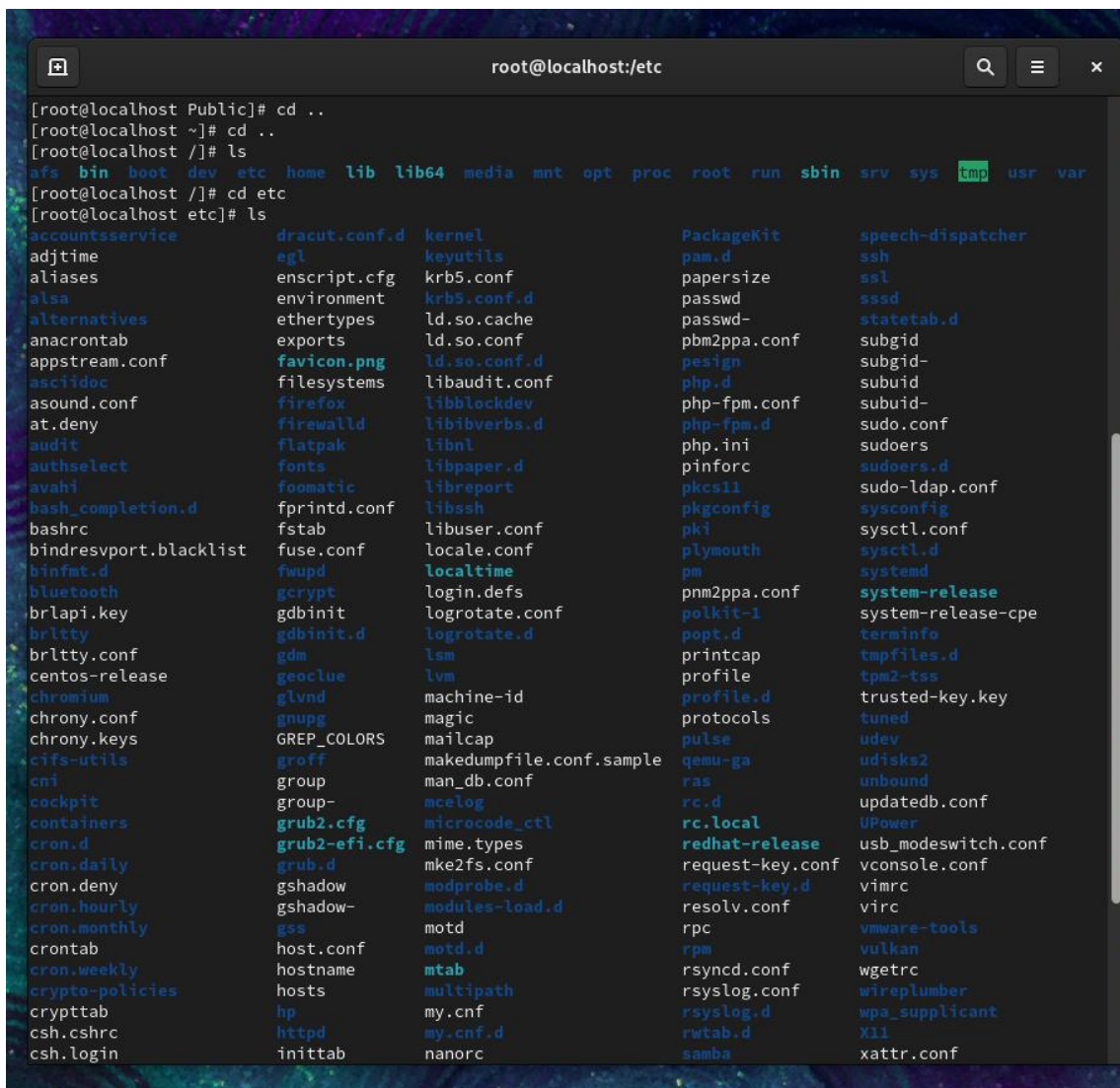


Imagen 105 Dirección /etc/zabbix/zabbix_server.conf para conImagenr base de datos de zabbix. [Fuente Propia]

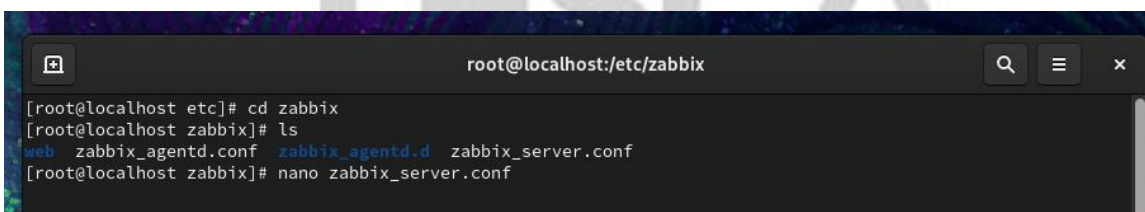


Imagen 106 Dirección /etc/zabbix/zabbix_server.conf para conImagenr base de datos de zabbix imagen 2. [Fuente Propia]

Imagen 106

Edita la siguiente sentencia con la contraseña establecida para el usuario en la base de datos de zabbix. El usuario es **zabbix@localhost**:

DBPassword=password

```

root@localhost:/etc/zabbix — nano zabbix_server.conf
GNU nano 5.6.1 zabbix_server.conf Modified
# DBSchema=

### Option: DBUser
# Database user.
#
# Mandatory: no
# Default:
# DBUser=
DBUser=root

### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password

### Option: DBSocket
# Path to MySQL socket.
#
# Mandatory: no
# Default:
# DBSocket=

### Option: DBPort
# Database port when not using local socket.
# If the Net Service Name connection method is used to connect to Oracle database, the port number from
# tnsnames.ora file will be used. The port number set here will be ignored.
#
# Mandatory: no
# Range: 1024-65535
# Default:
# DBPort=

### Option: AllowUnsupportedDBVersions
# Allow server to work with unsupported database versions.
# 0 - do not allow
# 1 - allow
#
# Mandatory: no
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo

```

Imagen 107 Asignando la contraseña de la base de datos de zabbix en la configuración. [Fuente Propia]

Iniciar Zabbix Server y el proceso de agente

```
# systemctl restart zabbix-server zabbix-agent httpd php-fpm
```

```
# systemctl enable zabbix-server zabbix-agent httpd php-fpm
```

```

root@localhost:/etc/zabbix
[root@localhost etc]# cd zabbix
[root@localhost zabbix]# ls
web  zabbix_agentd.conf  zabbix_agentd.d  zabbix_server.conf
[root@localhost zabbix]# nano zabbix_server.conf
[root@localhost zabbix]#
[root@localhost zabbix]#
[root@localhost zabbix]# systemctl restart zabbix-server zabbix-agent httpd php-fpm
[root@localhost zabbix]# systemctl enable zabbix-server zabbix-agent httpd php-fpm
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /usr/lib/systemd/system/zabbix-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /usr/lib/systemd/system/zabbix-agent.service.
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/php-fpm.service → /usr/lib/systemd/system/php-fpm.service.
[root@localhost zabbix]#
    
```

Imagen 108 Iniciando el servicio de Zabbix. [Fuente Propia]

Entrar a Zabbix Server por web frontend, existen tres opciones:

- 1) `http://host/zabbix`
- 2) `localhost/zabbix`
- 3) `dirección_ip_del_ordenador/zabbix`

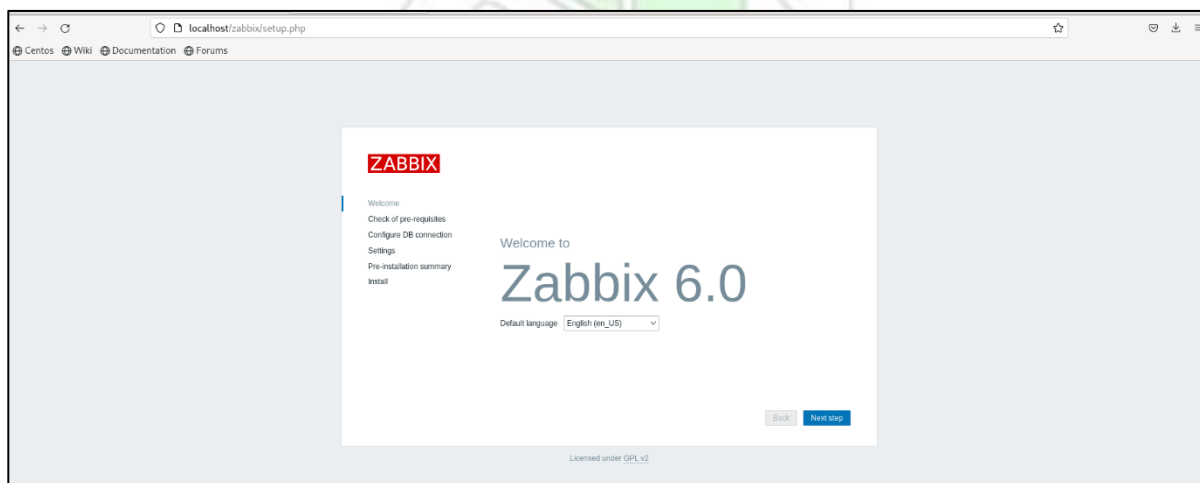


Imagen 109 Página de inicio de configuración de Zabbix Web. [Fuente Propia]

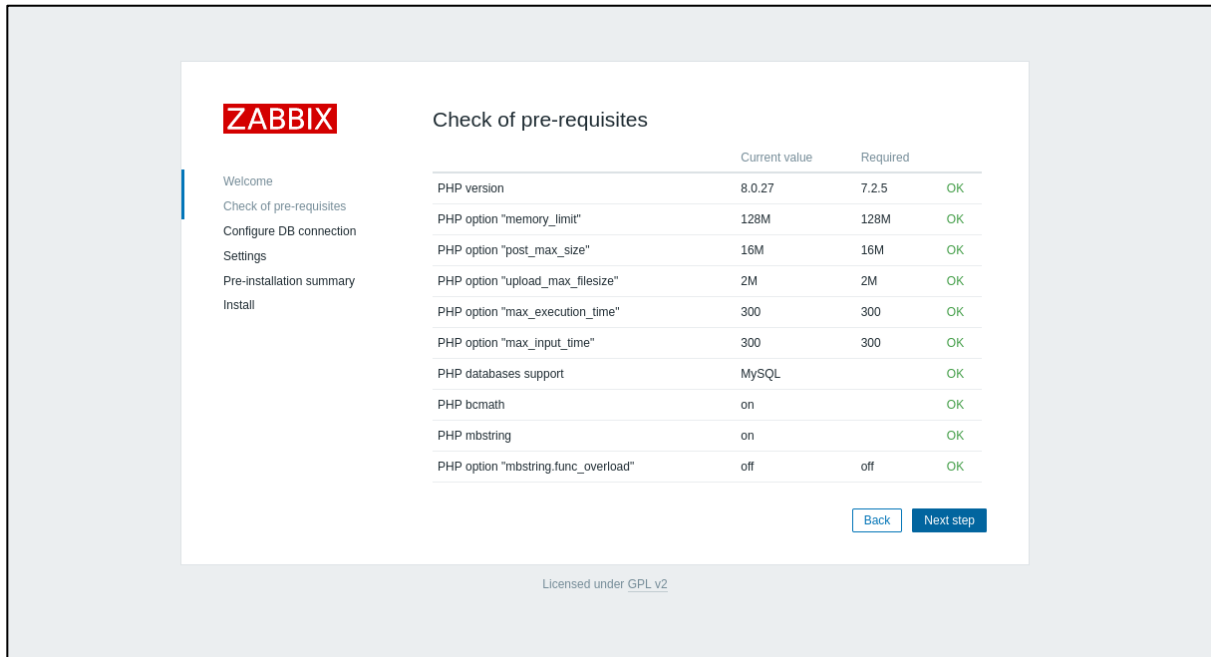


Imagen 110 Página de inicio de configuración de Zabbix Web imagen 2. [Fuente Propia]

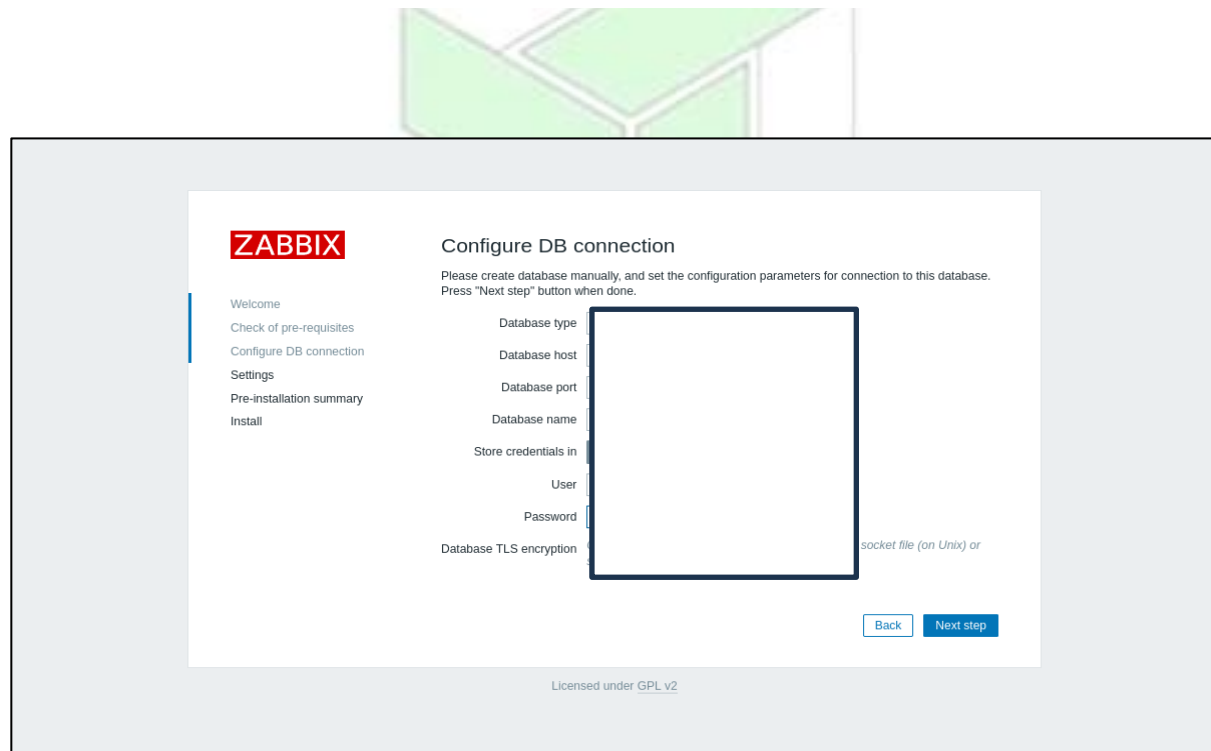
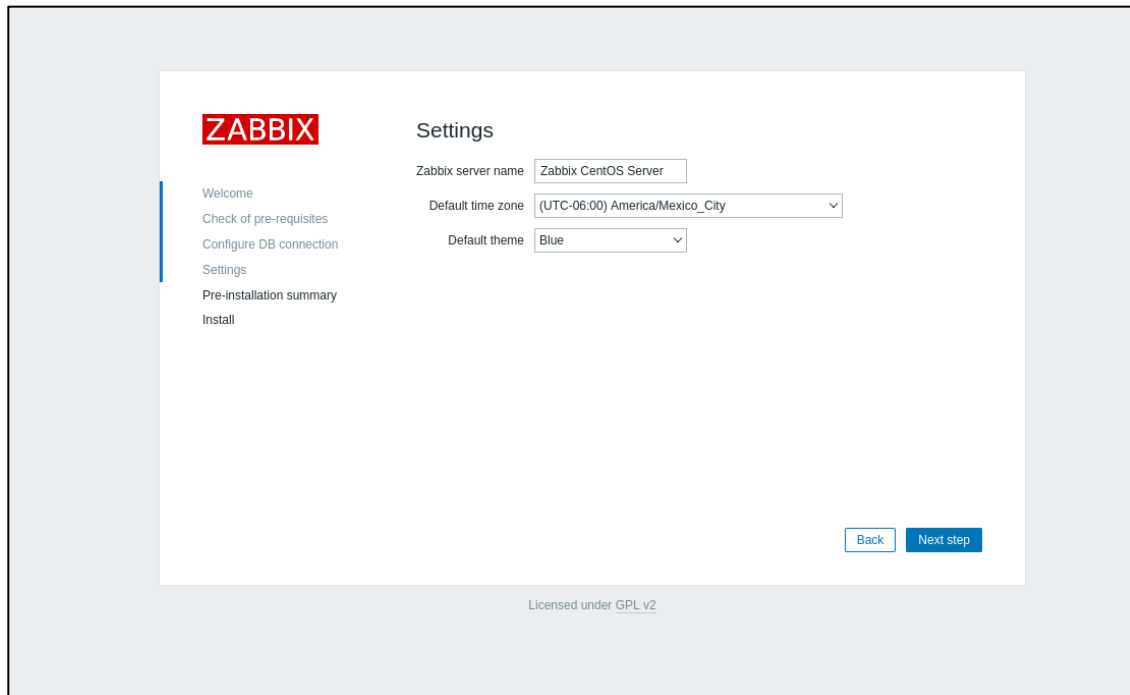


Imagen 111 Página de inicio de configuración de Zabbix Web imagen 3. [Fuente Propia]



ZABBIX

Settings

Welcome

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

Zabbix server name: Zabbix CentOS Server

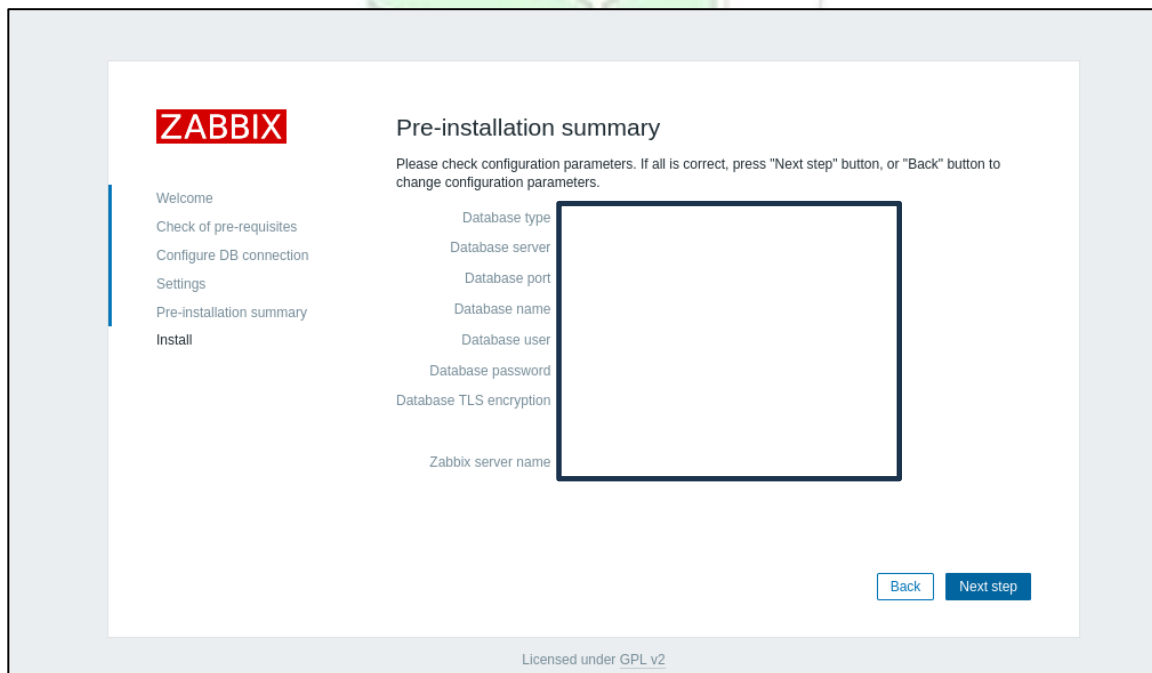
Default time zone: (UTC-06:00) America/Mexico_City

Default theme: Blue

Back Next step

Licensed under [GPL v2](#)

Imagen 112 Página de inicio de configuración de Zabbix Web imagen 4. [Fuente Propia]



ZABBIX

Pre-installation summary

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type

Database server

Database port

Database name

Database user

Database password

Database TLS encryption

Zabbix server name

Back Next step

Licensed under [GPL v2](#)

Imagen 113 Página de inicio de configuración de Zabbix Web imagen 5. [Fuente Propia]

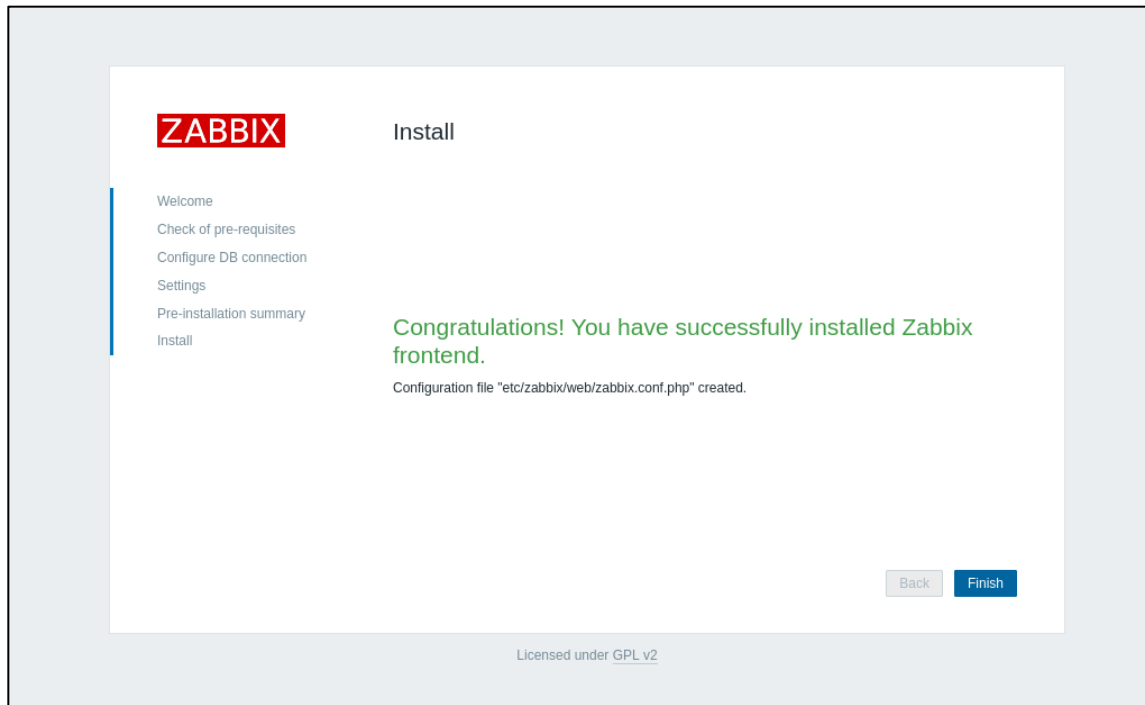


Imagen 114 Página de inicio de configuración de Zabbix Web imagen 6.[Fuente Propia]

Ingresa al web de zabbix es necesario entrar con usuario: Admin

Contraseña: zabbix

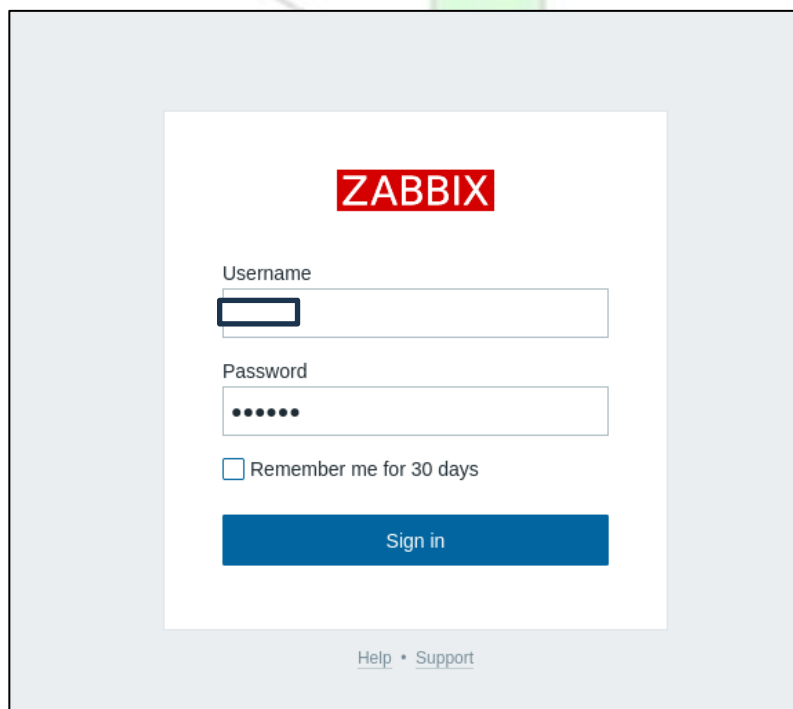


Imagen 115 Inicio de sesión de Zabbix Web. .[Fuente Propia]

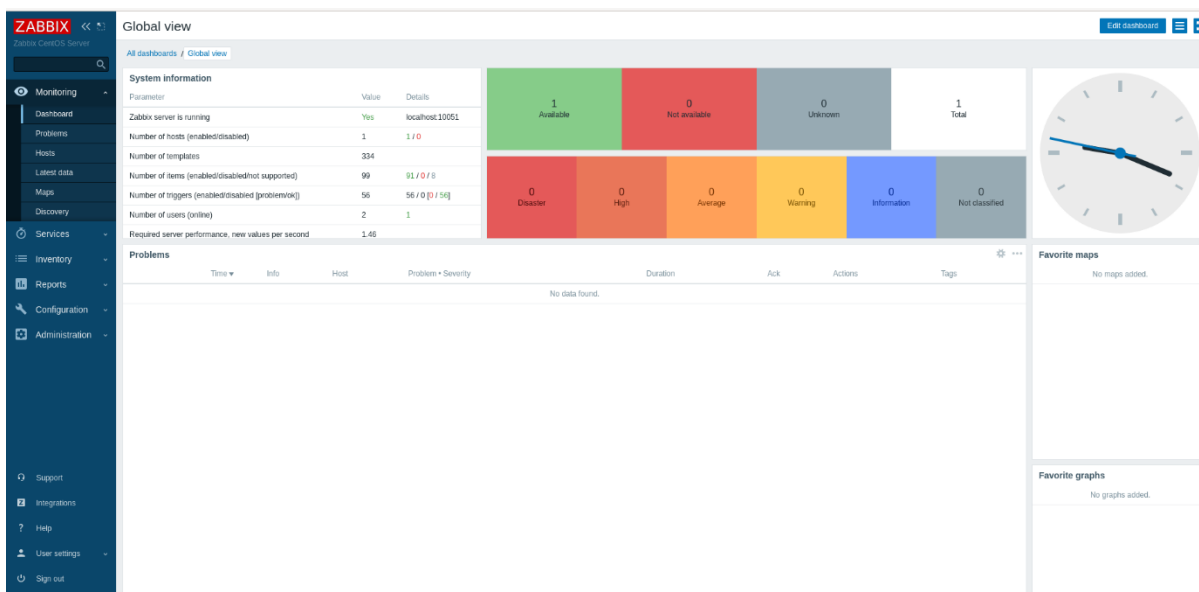


Imagen 116 Dashboard por defecto de Zabbix Web. .[Fuente Propia]

Implementación de ICMP

ICMP es un protocolo de red usado por dispositivos de red para diagnosticar si existen problemas de comunicación, por ejemplo, si los datos alcanzan o llegan a su destino y en qué tiempo se hace.

Este protocolo envía un mensaje de error a la fuente original donde fue enviada la información, ya sea porque hay mal conexión, se ha perdido datos o el paquete de datos es muy grande. Otra utilidad es saber y mostrar la ruta por la que pasan los paquetes a través de diferentes routers y dispositivos antes de llegar a su destino.

Ahora la implementación de ICMP a través de Zabbix se ha realizado de la siguiente manera:

Paso 1: Conectar en red servidor y ordenadores

El departamento de TICs a proporcionado un switch modelo SF1 10D-08 CISCO para conectar en red el servidor Zabbix con dos ordenadores. La red a la que se ha conectado pertenece a un switch que brinda servicio a los departamentos de administración, contabilidad, jurídico y superintendencia.

En la siguiente imagen se observa los tres dispositivos conectados. Al estar conectado a la intranet de CFE se les asigna por DHCP una dirección IP:



*Imagen 117 Puertos servidor y ordenadores conectados en red.
[Fuente Propia]*

Direcciones IP:

Servidor

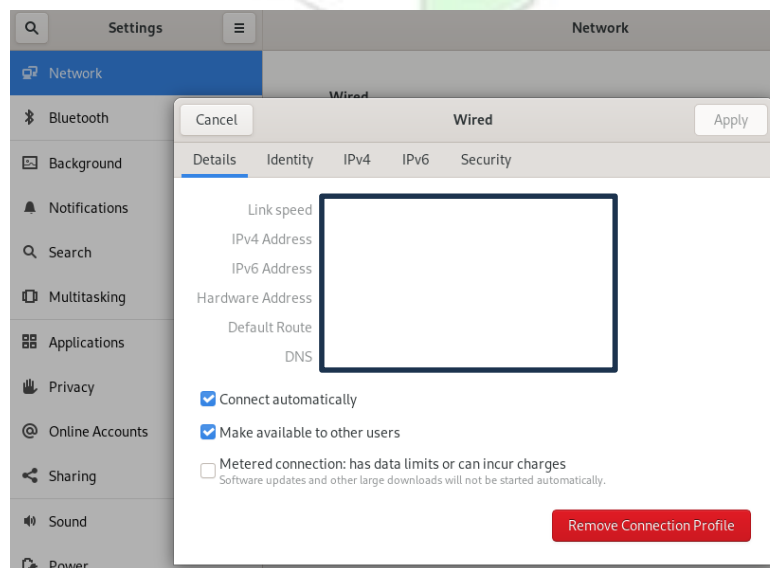


Imagen 118 Dirección IP servidor. [Fuente Propia]

Ordenador 1

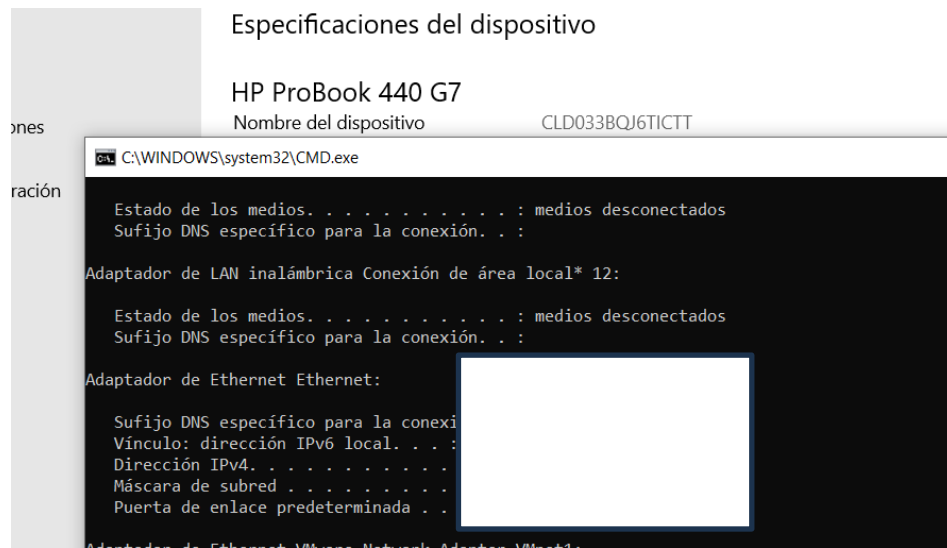


Imagen 119 Dirección IP ordenador1. [Fuente Propia]

Ordenador 2

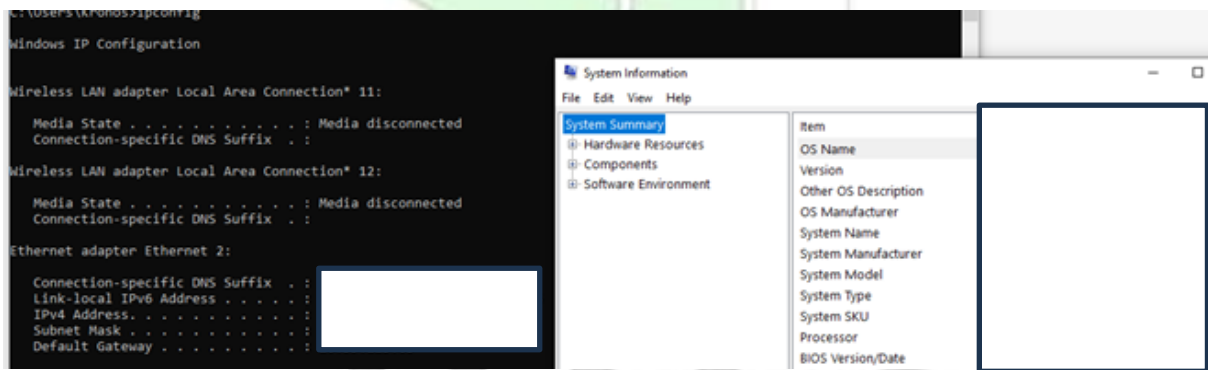


Imagen 120 Dirección IP ordenador2. [Fuente Propia]

Se comprueba la conectividad por ping

Ordenador 1 a servidor

```
C:\Users\TICTT>
C:\Users\TICTT>
C:\Users\TICTT>
C:\Users\TICTT>ping [redacted]

Haciendo ping a [redacted] con 32 bytes de datos:
Respuesta desde [redacted] bytes=32 tiempo=3ms TTL=64
Respuesta desde [redacted] bytes=32 tiempo=2ms TTL=64
Respuesta desde [redacted] bytes=32 tiempo=3ms TTL=64
Respuesta desde [redacted] bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para [redacted]
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 2ms, Máximo = 3ms, Media = 2ms
```

Imagen 121 Ping ordenador 1 a servidor. [Fuente Propia]

Ordenador 2 a servidor

```
C:\Users\Kronos>ping 10.59.113.106

Pinging [redacted] 32 bytes of data:
Reply from [redacted] bytes=32 time<1ms TTL=64
Reply from [redacted] bytes=32 time<1ms TTL=64
Reply from [redacted] bytes=32 time<1ms TTL=64
Reply from [redacted] bytes=32 time<1ms TTL=64

Ping statistics for [redacted]
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Imagen 122 Ping ordenador 2 a servidor. [Fuente Propia]

Entrar a Zabbix Server con la siguiente dirección localhost/zabbix en el navegador web

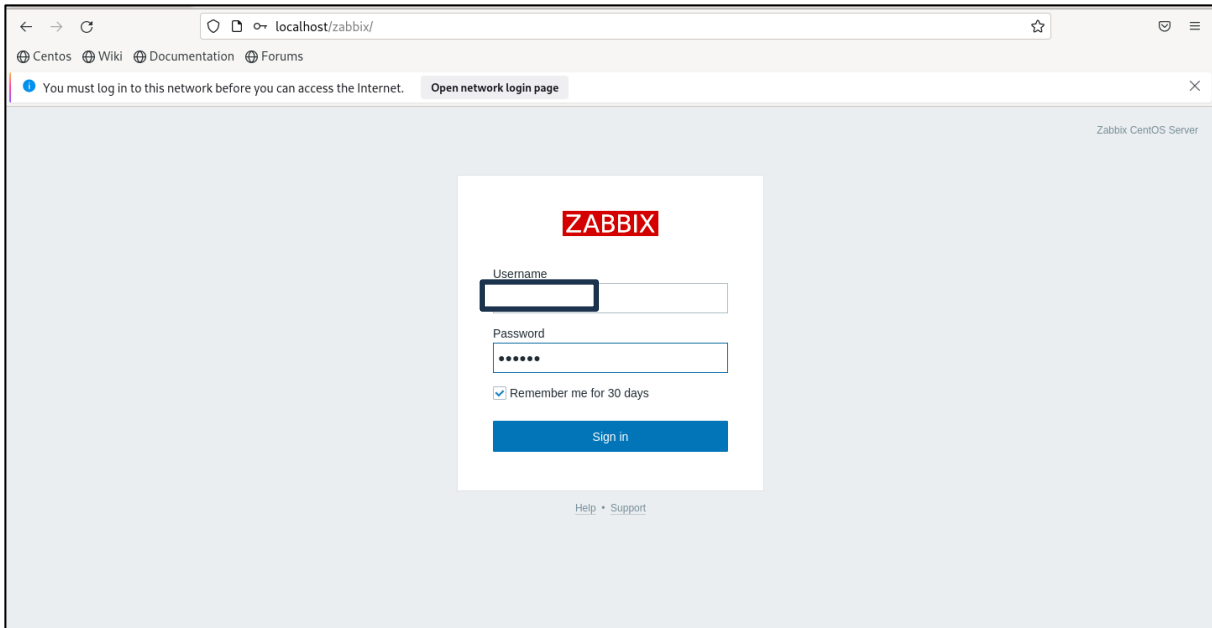


Imagen 123 Entrando a zabbix web. [Fuente Propia]

Crear un HostGroup

El hostgroup permitirá organizar y separar por departamentos los ordenadores. Para crear una ingresa a Configuration en el menú izquierdo y selecciona Create host group en Host Groups:

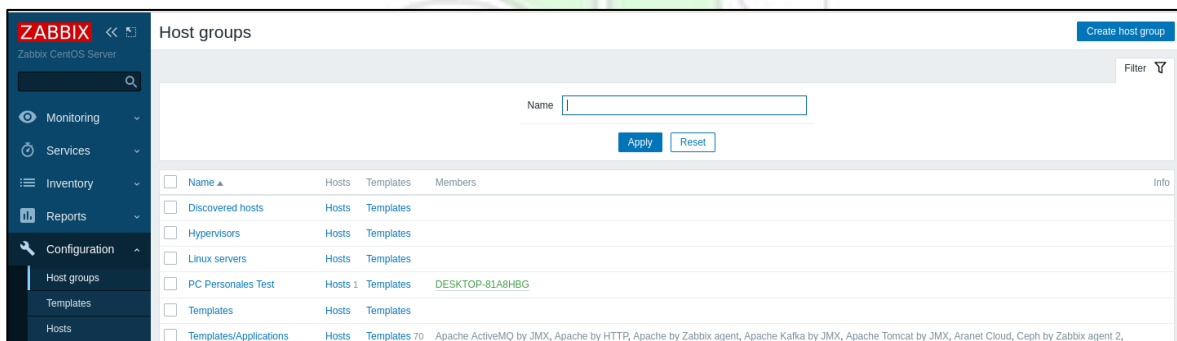


Imagen 124 Botón Create host group. [Fuente Propia]

Nombramos el grupo de computadoras, ejemplo “Departamento TICs”, y agregamos:

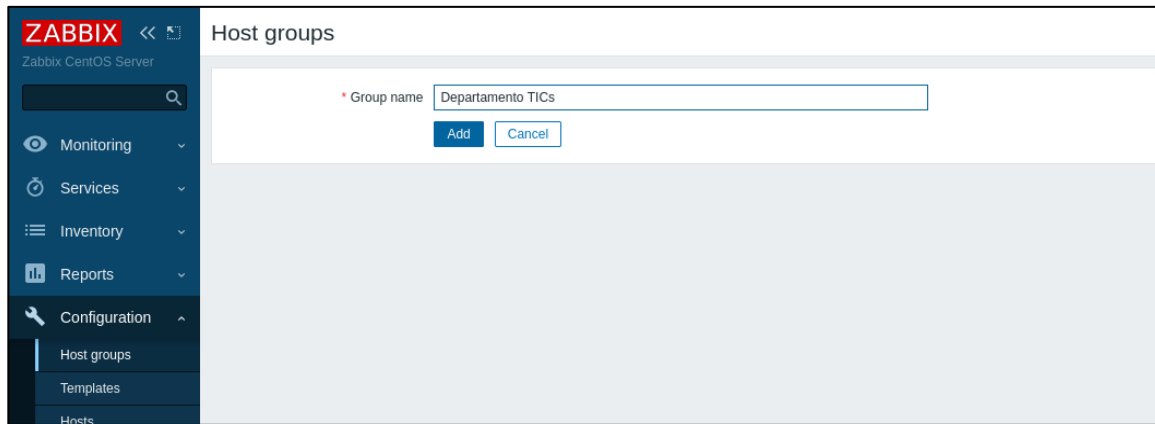


Imagen 125 Nombre host group. [Fuente Propia]

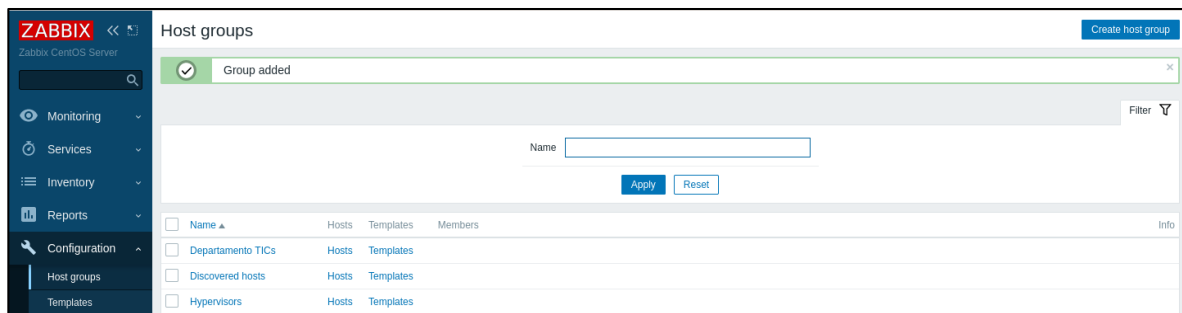


Imagen 126 Host group added. [Fuente Propia]

Creación de Host

Se creo el host (ordenador a monitorear) en el menú izquierdo en la pestaña Configuration>Hosts y en la parte superior derecha en el botón Create Host:

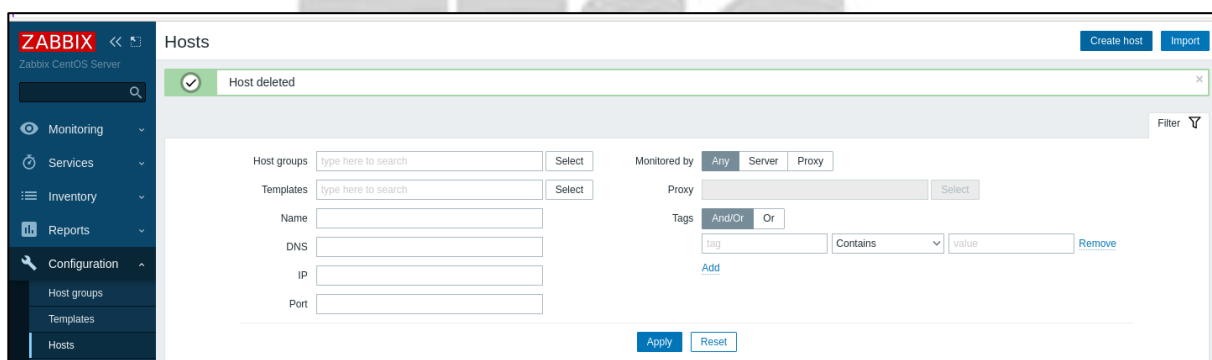


Imagen 127 Botón Create Host. [Fuente Propia]

Se agrega el nombre del primer ordenador el cual es CLD033BQJ6TICTT, la plantilla (template) de ICMP y el HostGroup al que pertenece:

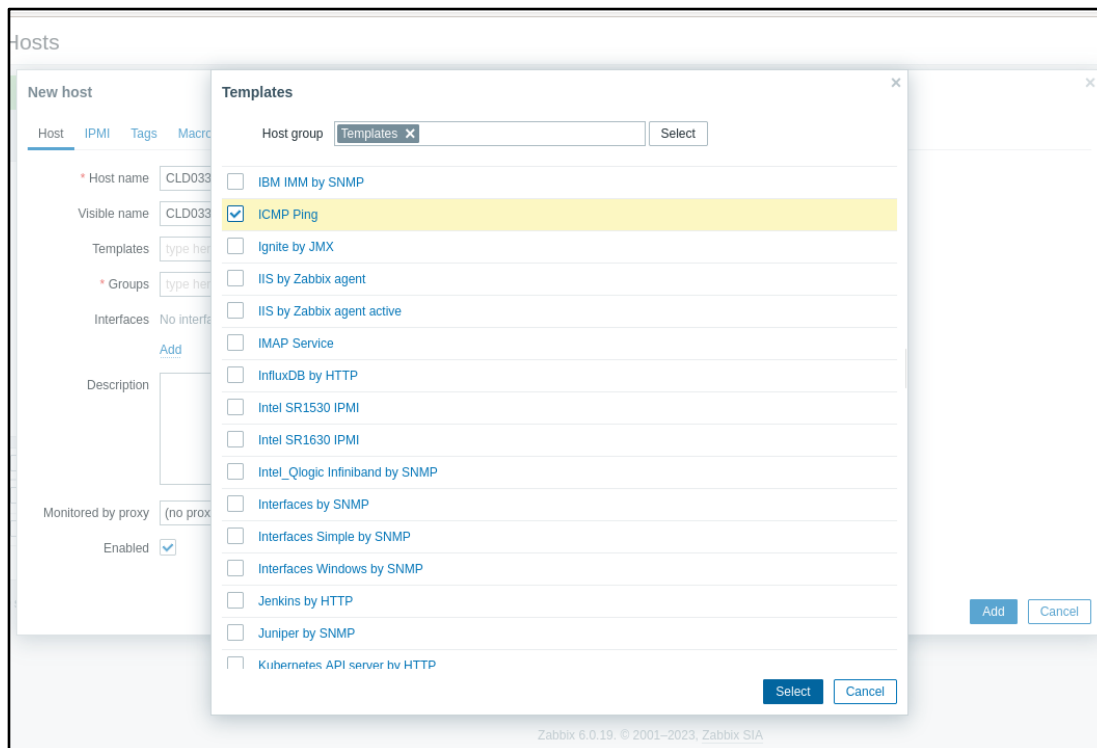


Imagen 128 Agregando un template ICMP. [Fuente Propia]

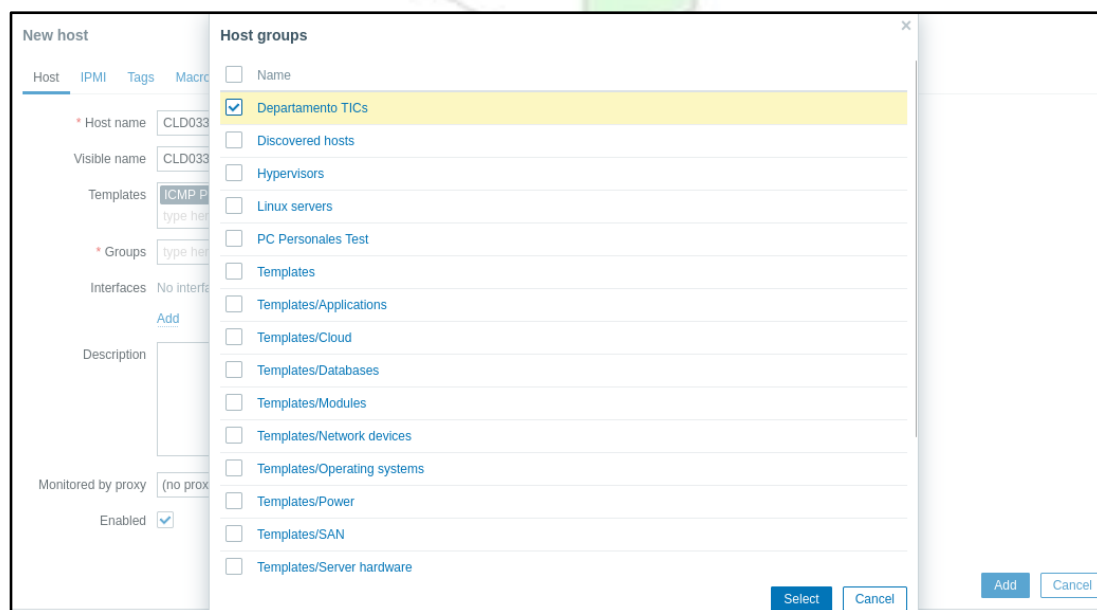


Imagen 129 Agregando un template ICMP a un host group. [Fuente Propia]

Se agrego un agente (no es un agente instalado, toma la dirección del ordenador como un agente) con la dirección IP del ordenador 1:

Imagen 130 Agregando un agent al host. [Fuente Propia]

Imagen 131 Información del host para agregar. [Fuente Propia]

Monitoreo

Ha sido añadido el ordenador, se puede visualizar la información proporcionada por ICMP como la pérdida de paquetes, disponibilidad y el tiempo de respuesta

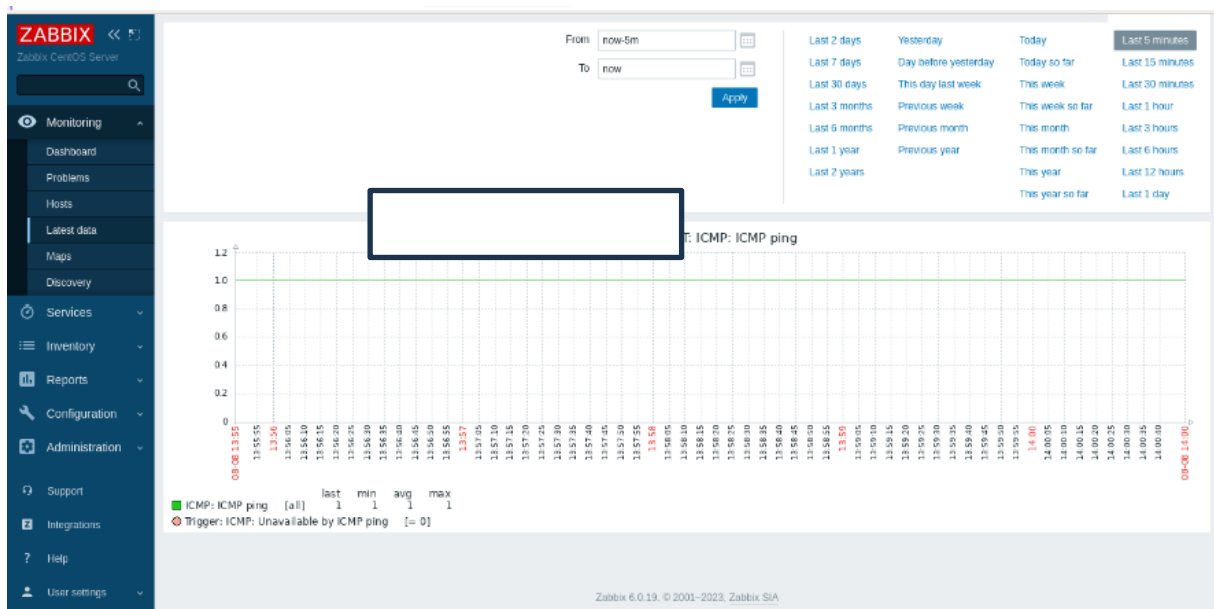


Imagen 132 Grafica ICMP ping. [Fuente Propia]

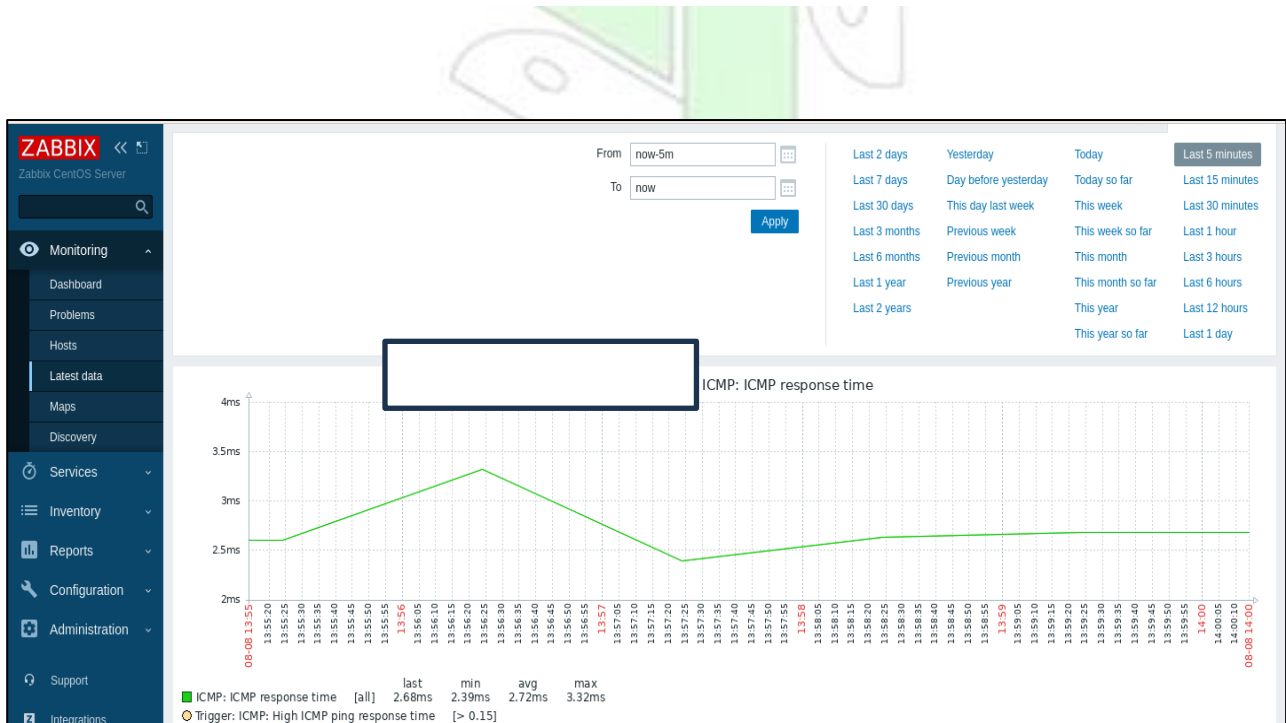


Imagen 133 Grafica ICMP response time. [Fuente Propia]

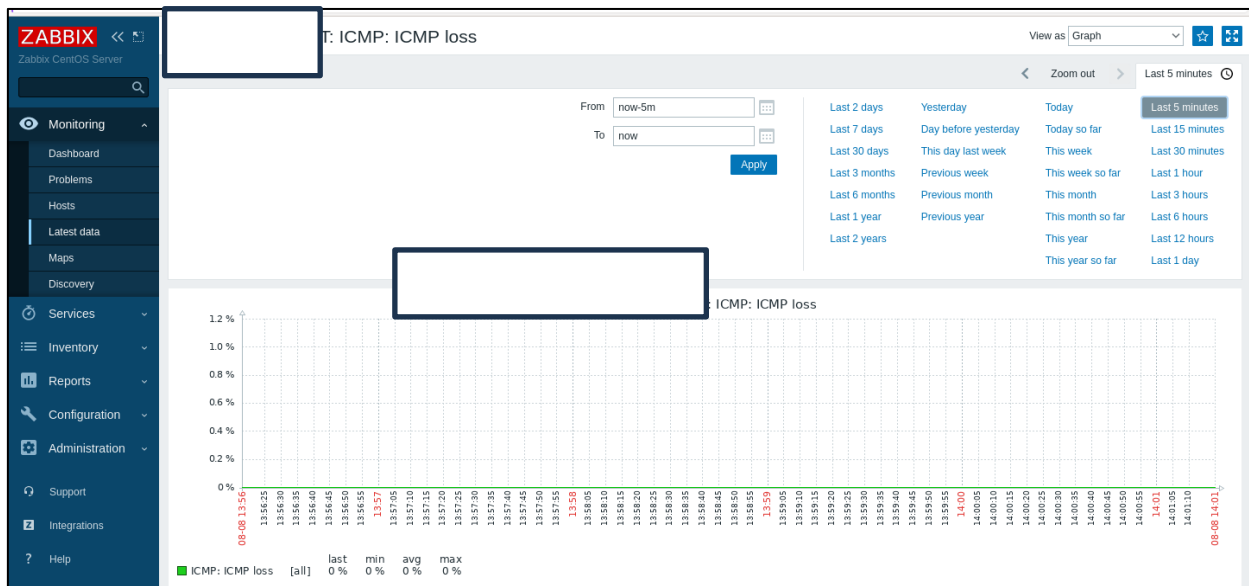


Imagen 134 Grafica ICMP los. [Fuente Propia]

Prueba de desconectar el ordenador de la red en las gráficas y al reconectar los cambios de nuevo:

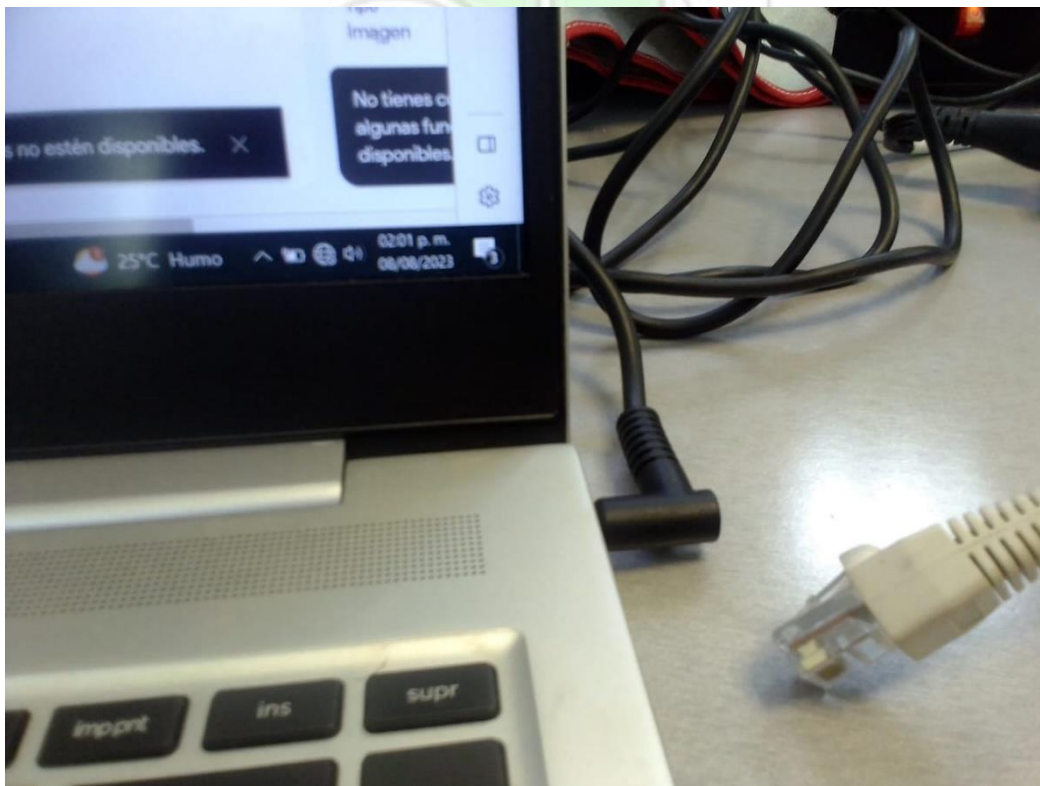


Imagen 135 Puerto ethernet desconectado ordenador 1. [Fuente Propia]



Imagen 136 Puerto ethernet reconectado ordenador 1. [Fuente Propia]



Imagen 137 Grafica ICM loss después de reconexión. [Fuente Propia]

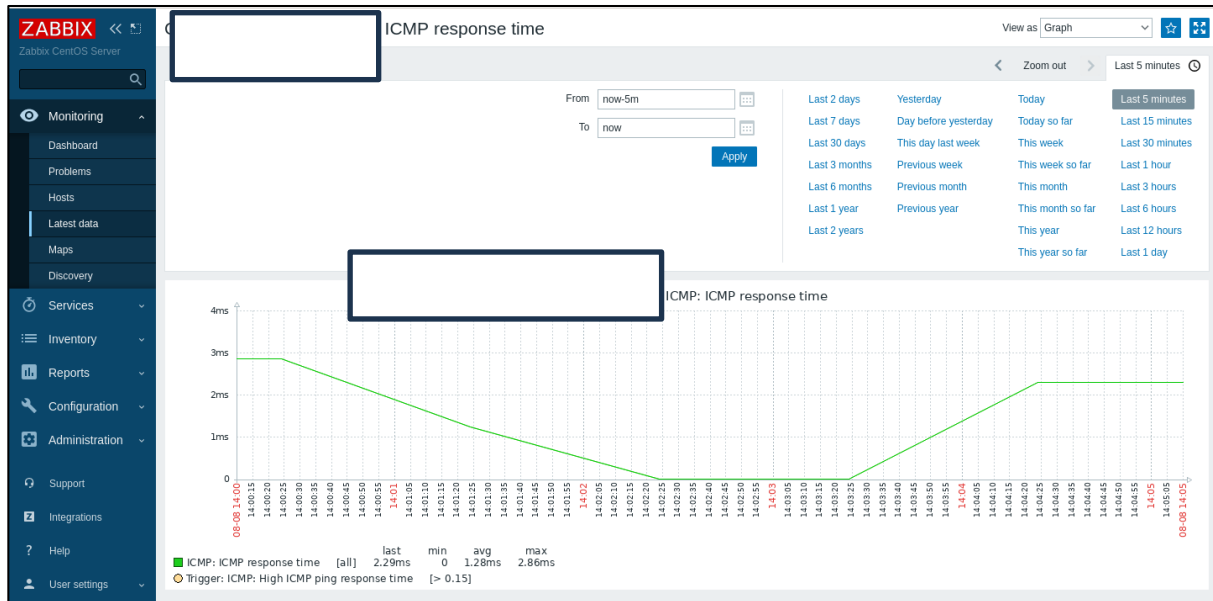


Imagen 138 Grafica ICM response time después de reconexión. [Fuente Propia]

Se repite el proceso con el ordenador 2, además se observó al desconectar el equipo de la red, un warning de incidente, así mismo, al reconectar se advierte la solvencia del problema.

The figure shows the Zabbix 'Host' configuration form. The 'Host' tab is selected, showing fields for 'Host name' (empty), 'Visible name' (empty), 'Templates' (set to 'ICMP Ping'), and 'Groups' (set to 'Departamento TICs'). The 'Interfaces' section shows a single interface with 'Agent' type, IP address '10.59.113.75', and port '10050'. The 'Description' field is empty. The 'Monitored by proxy' dropdown is set to '(no proxy)'. The form includes buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'. The sidebar on the left shows navigation options like Monitoring, Services, and Configuration. The top bar includes search and view settings.

Imagen 139 Creación de host 2 del ordenador 2. [Fuente Propia]

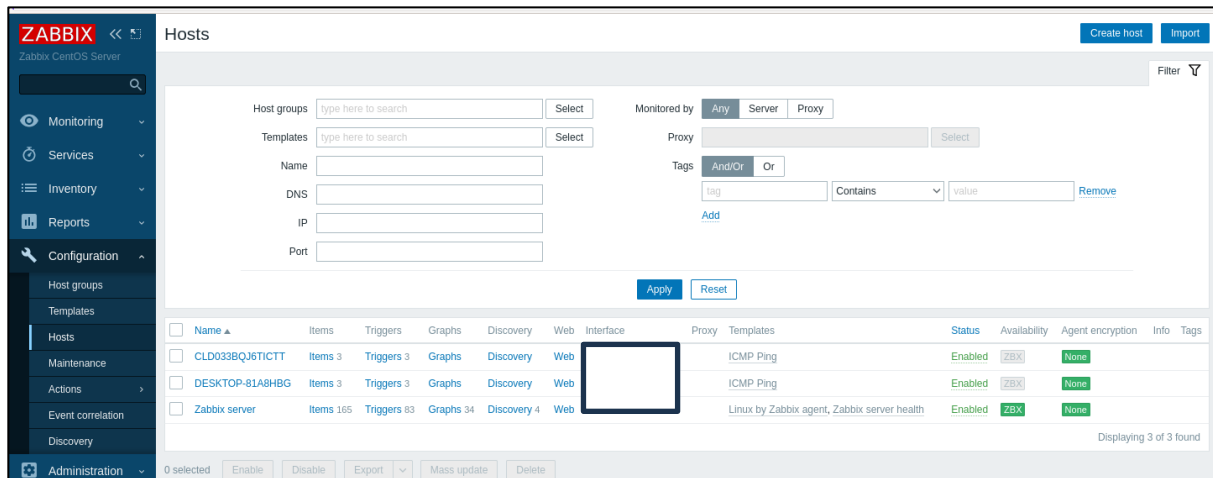


Imagen 140 Visualización de agregado del ordenador 2. [Fuente Propia]

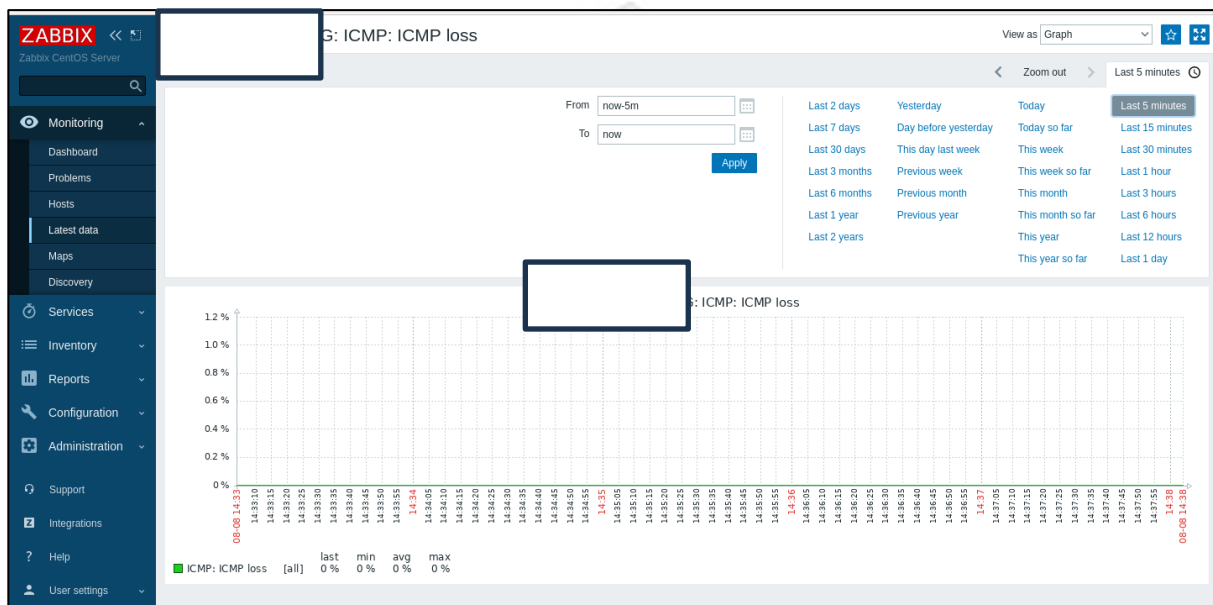


Imagen 141 Grafica ICMP loss ordenador 2. [Fuente Propia]

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

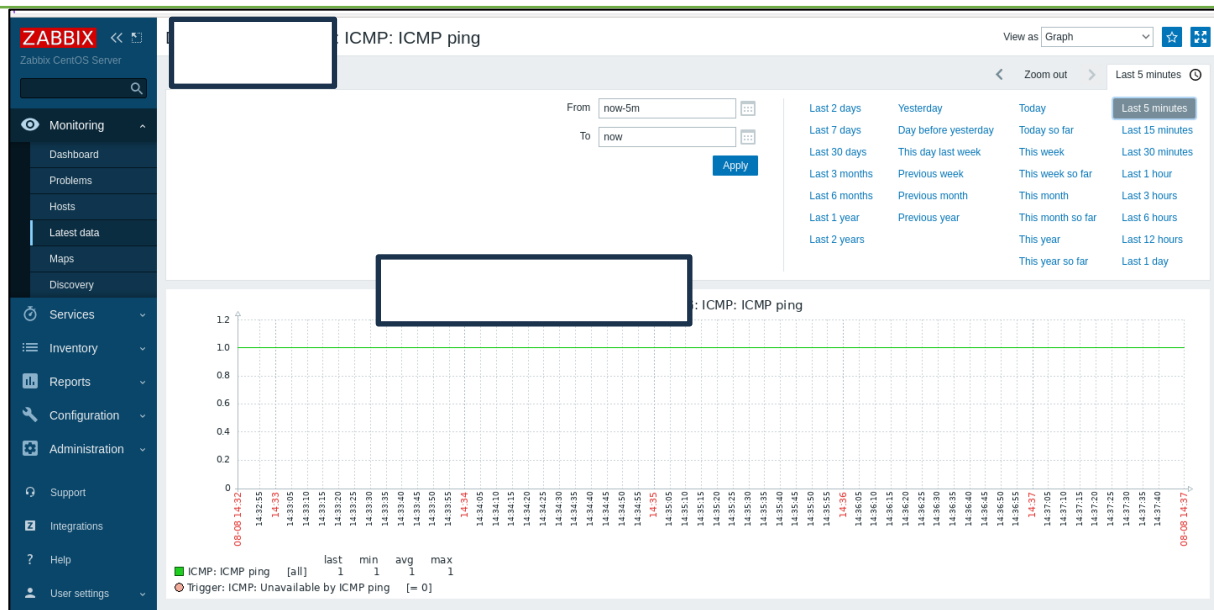


Imagen 142 Grafica ICMP ping ordenador 2. [Fuente Propia]

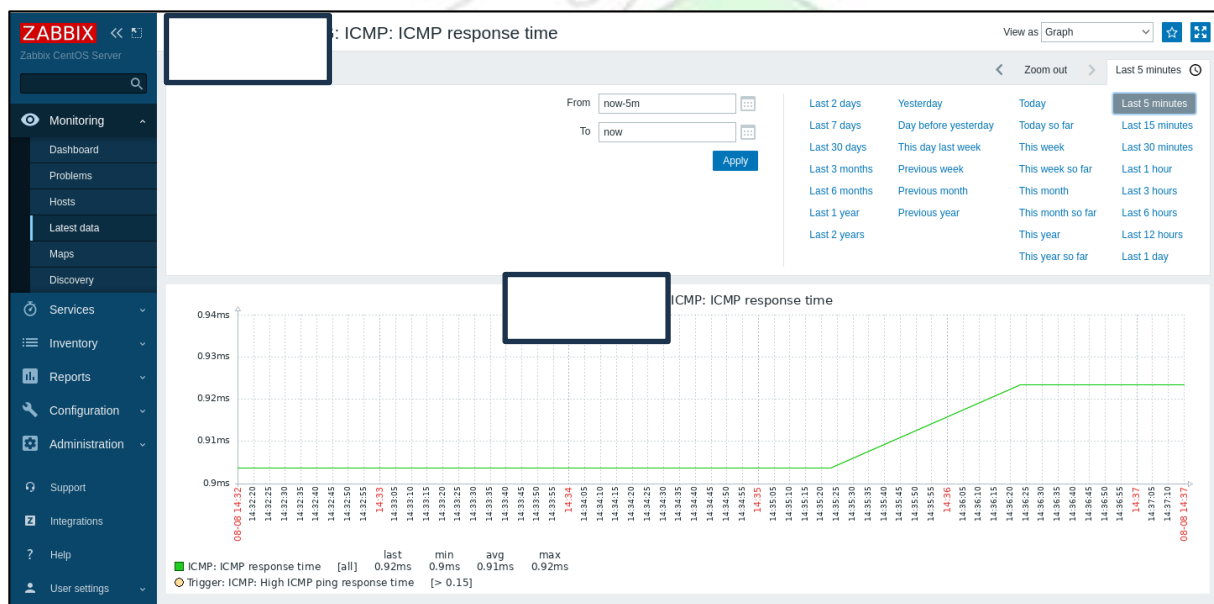


Imagen 143 Grafica ICMP response time ordenador 2. [Fuente Propia]



Imagen 144 Puerto ethernet desconectado del ordenador 2. [Fuente Propia]

The screenshot shows the Zabbix web interface. On the left is a sidebar with navigation links: Monitoring, Dashboard, Problems, Hosts, Latest data, Maps, Discovery, Services, Inventory, Reports, Configuration, Administration, and Support. The main content area is titled 'Problems' and includes search filters for Host groups, Hosts, Triggers, Problem, Severity, and Age. Below the filters is a table of problems. The first row shows a problem at 14:41:23 with a 'High' severity, labeled 'PROBLEM'. The problem details indicate 'ICMP: Unavailable by ICMP ping' with a duration of 10s and status 'No'. The tags include 'component: health', 'component: network', and 'scope: availability'.

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
14:41:23	High		PROBLEM			↑ ICMP: Unavailable by ICMP ping	10s	No		component: health component: network scope: availability

Imagen 145 Warning de puerto ethernet desconectado del ordenador 2. [Fuente Propia]

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Subfilter affects only filtered data

HOSTS:

TAGS: component 3

TAG VALUES: component: health 3 network 3

DATA: With data Without data

☐	Host	Name ▲	Last check	Last value	Change	Tags	Info
☐		ICMP: ICMP loss	8s	100 %		component: health component: network	Graph
☐		ICMP: ICMP ping	8s	Down (0)		component: health component: network	Graph
☐		ICMP: ICMP response time	8s	0		component: health component: network	Graph

Displaying 3 of 3 found

Imagen 146 Cambio de los datos por la desconexión del puerto ethernet ordenador 2. [Fuente Propia]



Imagen 147 Reconexión del puerto ethernet ordenador 2. [Fuente Propia]

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

The screenshot shows the Zabbix 'Problems' page. The left sidebar contains navigation links for Monitoring, Services, Inventory, Reports, Configuration, Administration, Support, Integrations, Help, and User settings. The main content area displays filters for Host groups, Hosts, Triggers, and Severity. A table of problems is shown with columns for Time, Severity, Recovery time, Status, Info, Host, Problem, Duration, Ack, Actions, and Tags. One problem is listed: 'ICMP: Unavailable by ICMP ping' with a status of 'RESOLVED' and a duration of '2m'. The problem is acknowledged and has tags 'component: health', 'component: network', and 'scope: availability'.

Imagen 148 Warning de problema resuelto de puerto ethernet ordenador 2. [Fuente Propia]

The screenshot shows the Zabbix 'Problem details' page for the problem 'ICMP: Unavailable by ICMP ping'. The page displays the host name, problem name, and a table of data points. The table has columns for Host, Name, Last check, Last value, Change, Tags, and Info. Three data points are shown: 'ICMP: ICMP loss' (0 %), 'ICMP: ICMP ping' (Up (1)), and 'ICMP: ICMP response time' (0.92ms). The problem is acknowledged and has tags 'component: health', 'component: network', and 'scope: availability'.

Imagen 149 Cambio de información por solvencia de problema de puerto ethernet ordenador 2. [Fuente Propia]

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

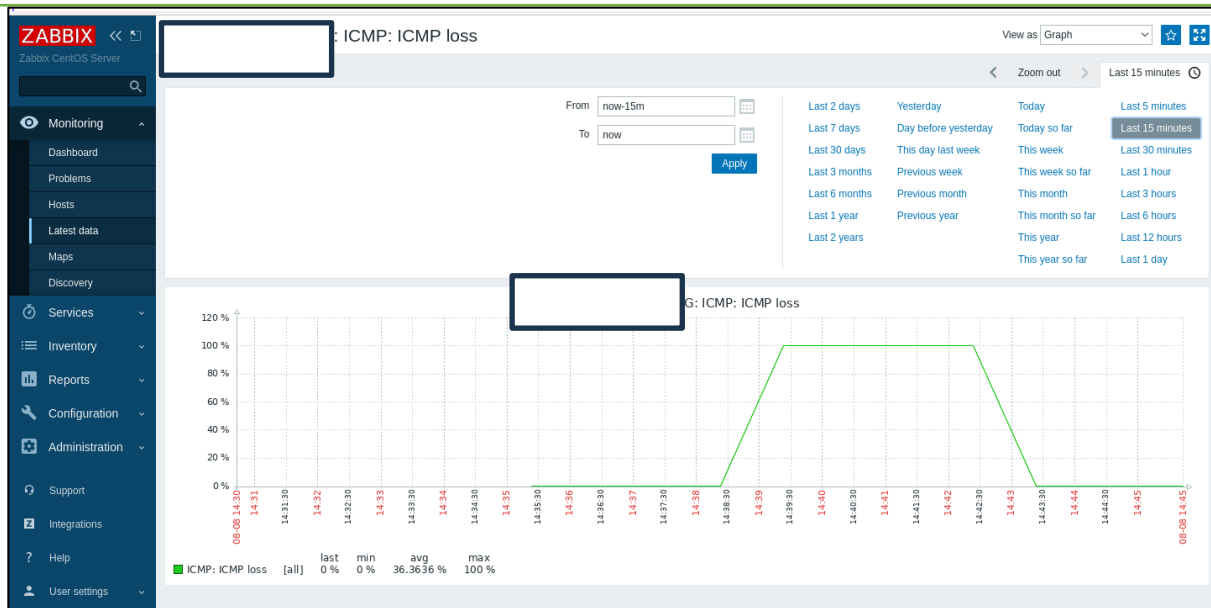


Imagen 150 Cambio en la gráfica ICMP loss ordenador 2. [Fuente Propia]



Imagen 151 Cambio en la gráfica ICMP ping ordenador 2. [Fuente Propia]

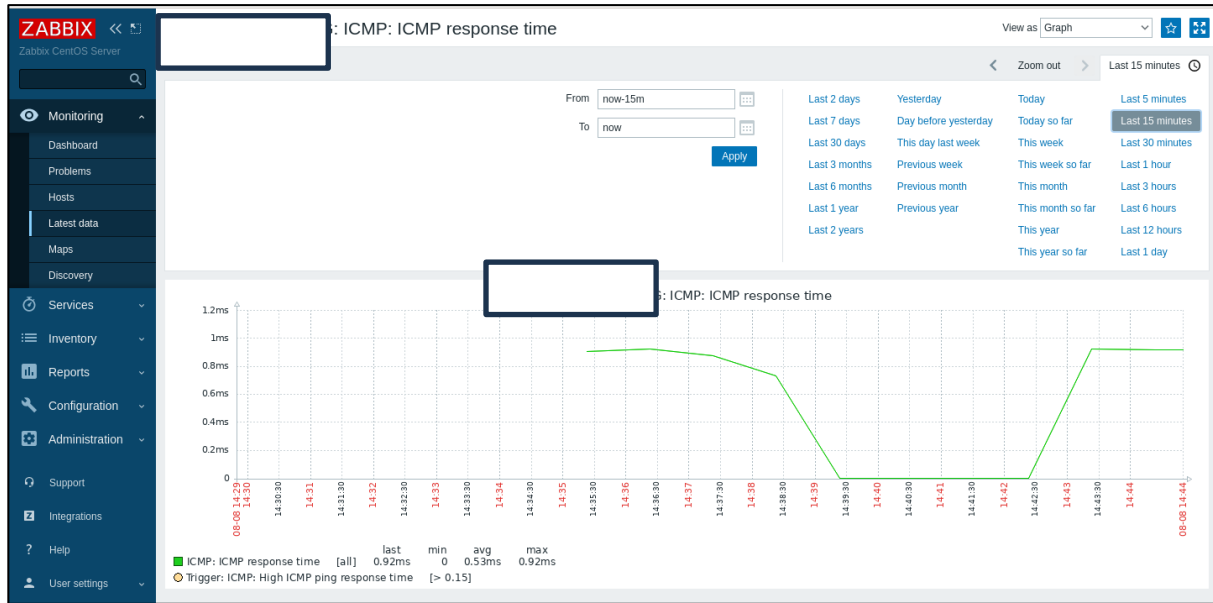


Imagen 152 Cambio en la gráfica ICMP response time ordenador 2. [Fuente Propia]



TESCO

4.1.4. ACTIVIDAD A REALIZAR

3.4 Realizar recomendaciones de uso de agentes para monitoreo de la red

DESCRIPCIÓN DE LA ACTIVIDAD

Recomienda el uso de agentes de Zabbix para ser instalados en ordenadores Windows y monitorear otros aspectos de estos equipos asignados a usuarios, se realizan pruebas para demostrar su función.

RESULTADO DE LA ACTIVIDAD

El protocolo ICMP con ayuda de la herramienta Zabbix, cumple al cien por ciento los requerimientos por parte de la empresa, permite conocer básicamente la disponibilidad, latencia y si hay o no paquetes que se estén perdiendo. Puede ser complementada para gran ayuda de la misma, por lo que a continuación se desarrollaron una serie de instrucciones del uso de agentes para ordenadores en de los usuarios con el fin de obtener mayor información, por ende, mayor control y prevención.

Recomendación de agentes de Zabbix sustituyendo SNMP

En conjunto con la empresa, se considera la implementación de SNMP en ordenadores de usuarios sería muy complejo de llevar a cabo debido a la obtención de MIBs, un mayor proceso de instalación en los equipos además de posibles vulnerabilidades generadas por este protocolo. Por lo que una mejor alternativa es el uso de agentes.

La norma ISO-IEC 27001:2013 página 18 Sección 10.2 Mejora continua establece La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información. A continuación, se sugiere para el monitoreo en la red al pasar la fase de autorización, la implementación de agentes lo cual significa gran escalabilidad para el monitoreo en la intranet de CFE Zona Cuautitlán. Nota: Para saber más diríjase al anexo A.5 ISO-IEC 27001:2013 Sección 10.2 Mejora continua

Información necesaria para Monitorear aspectos útiles para la organización acerca de sus usuarios y anticiparse a posibles vulnerabilidades en los equipos, esta recomendación sustituye el uso del protocolo SNMP y complementa la estrategia **A) Instalar y configurar un servidor y sus controles haciendo uso de software para el monitoreo del ping y protocolo SNMP en los equipos informáticos de la intranet de manera local en Zona Cuautitlán.**

Tabla 49 Información a monitorear para prueba de agentes. [Fuente Propia]

Información para monitorear/advertir					
Información	Se debe	Norma			
Errores Ethernet		Norma ISO-IEC 27001:2013			
		Anexo	Anexo	Anexo	Anexo
		A.12 Seguridad de las operaciones	A.12.4.1	Registro de eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información
Tiempo de uso		Norma ISO-IEC 27001:2013			
		Anexo	Proceso	Actividad	Control
		A.9 Control de acceso	A.9.1.2	Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados

Nota: Para saber más diríjase al anexo A.6 ISO-IEC 27001:2013 Anexo A.12 Seguridad de las operaciones

Nota: Para saber más diríjase al anexo A.7 ISO-IEC 27001:2013 Anexo A.9 Control de acceso

Paso 1: Conectar el servidor con los clientes

El servidor debe conectarse a los ordenadores de dónde obtendrá la información.

Por razones de seguridad y confidencialidad, se ha establecido una conexión LAN entre una laptop de prueba ASUS y el servidor Zabbix en Centos sin hacer uso de la intranet:



Imagen 153 Puertos de servidor y ordenador de prueba conectados. [Fuente Propia]

Para asegurar que existe la conexión se debió haber implementado el monitoreo por ICMP, se hizo hacer un ping del cliente al servidor y del servidor al cliente.

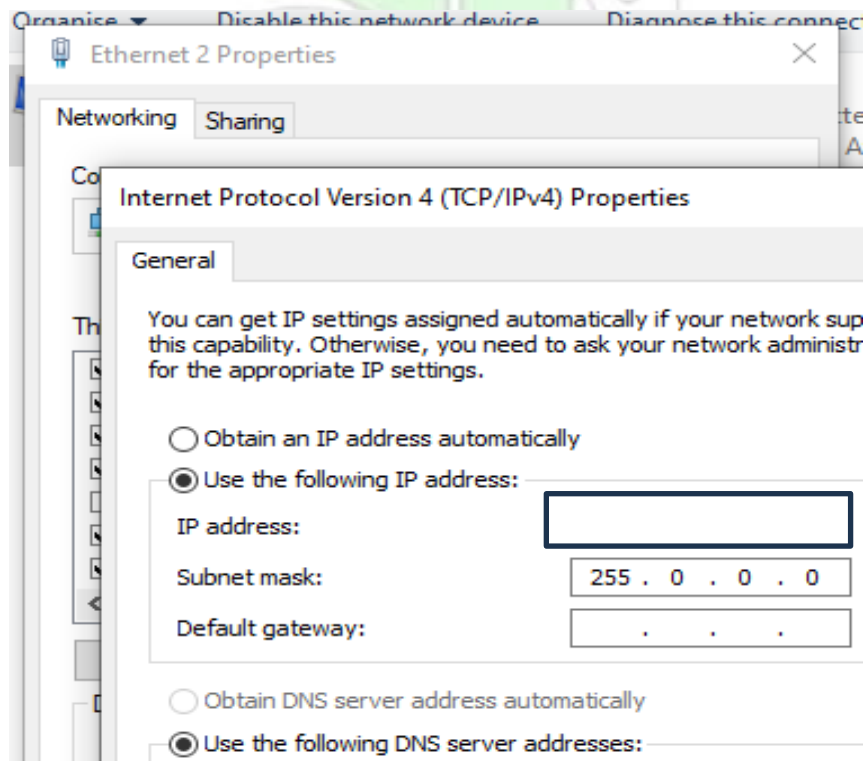


Imagen 154 Dirección IP asignada a ordenador de prueba. [Fuente Propia]

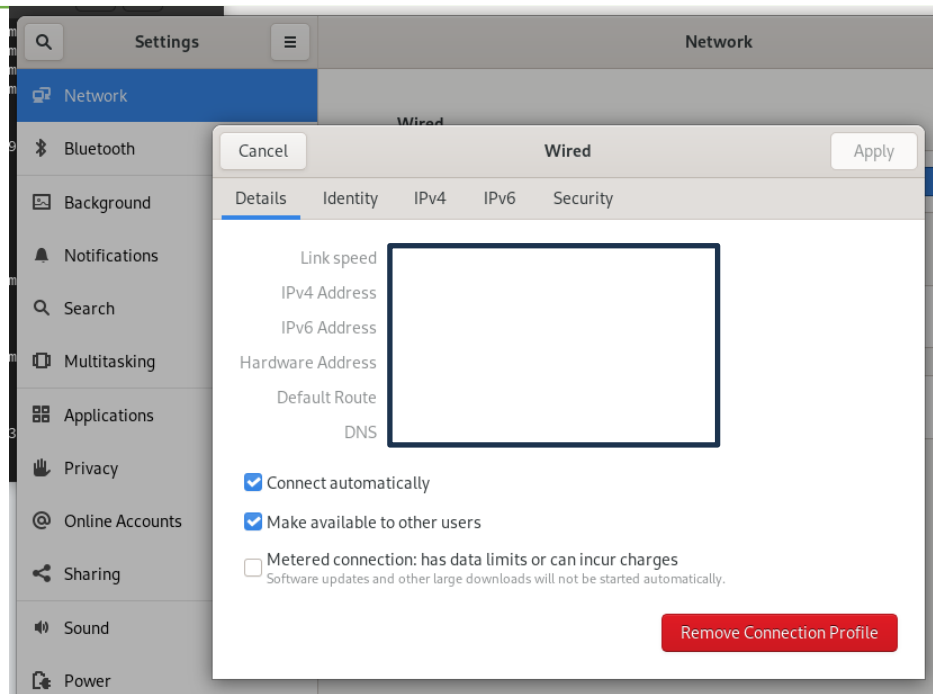


Imagen 155 Dirección IP asignada a servidor. [Fuente Propia]

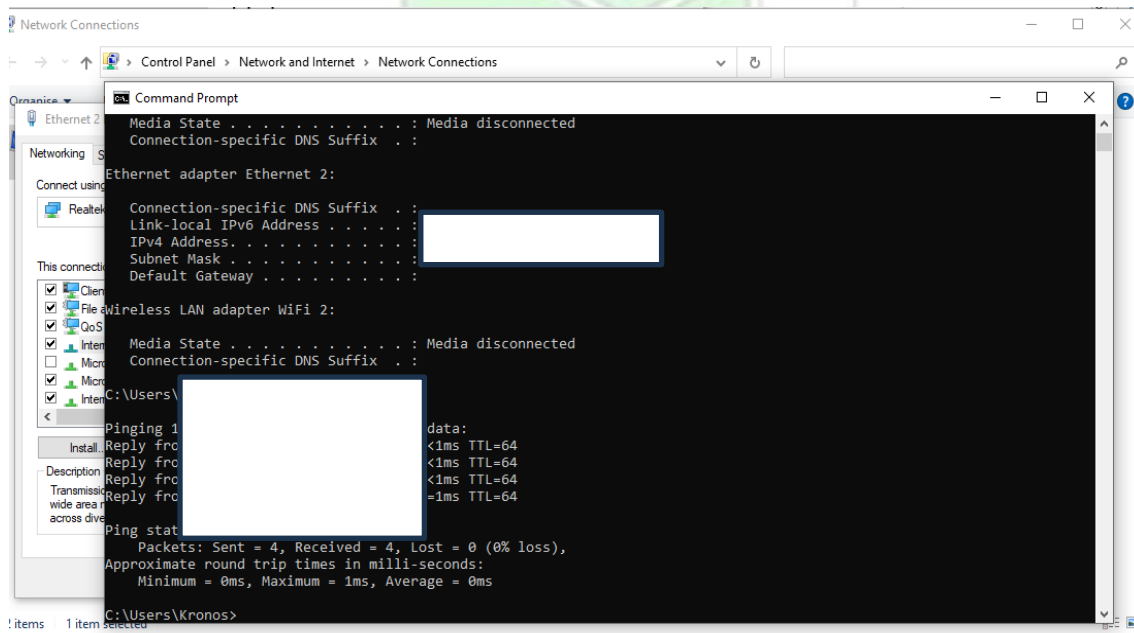


Imagen 156 Ping de ordenador de prueba a servidor. [Fuente Propia]

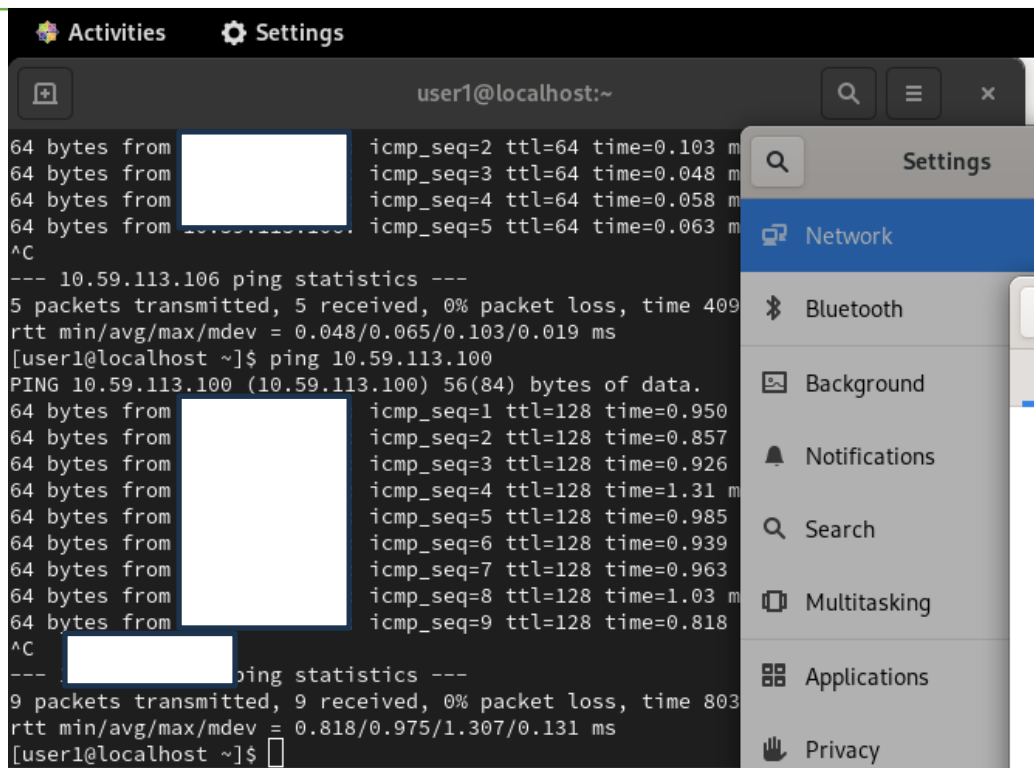


Imagen 157 Ping de servidor a ordenador de prueba. [Fuente Propia]

Paso 2: Instalar agente en ordenador Windows

Se descargó del ordenador Windows el agente de Zabbix, según las características del ordenador, para monitoreo de la página Oficial de Zabbix:



Imagen 158 Descarga del agente Zabbix para Windows. [Fuente Propia]

Se ha descargado para estas instrucciones de ejemplo, el agente disponible para la versión del servidor Zabbix 6.0:



Imagen 159 Descarga del agente Zabbix para Windows versión 6.0.19. [Fuente Propia]

Se ejecuto el archivo descargado, se aceptaron los términos.

Llegando a esta ventana de asistente, se escribieron los datos del nombre del ordenador (hostname), la dirección del servidor de Zabbix, el puerto por defecto es el 10050, Server or Proxy for active check igualmente la dirección IP del campo Zabbix Server IP/DNS y se agregó el agente a Add agente location to the PATH. Se recuerda que la configuración de una llave PSK, el no añadir el agente al PATH, diferente puerto o diferente dirección para proxy y server, será personalizada a lo establecido por la empresa al momento de la implementación.

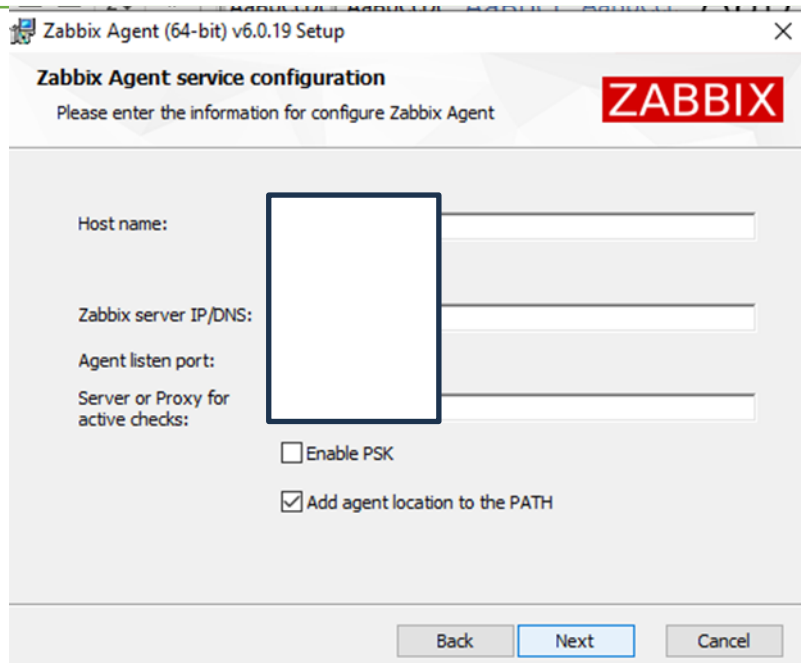


Imagen 160 Configuración de agente Zabbix por asistente para Windows. [Fuente Propia]

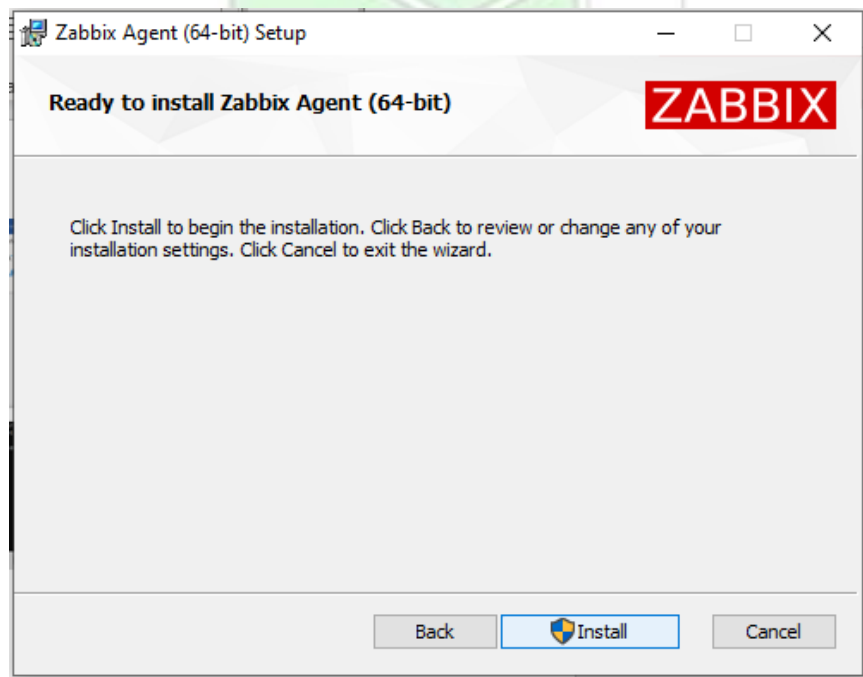


Imagen 161 Instalar Agente Zabbix en Windows. [Fuente Propia]

Finalizo la instalación

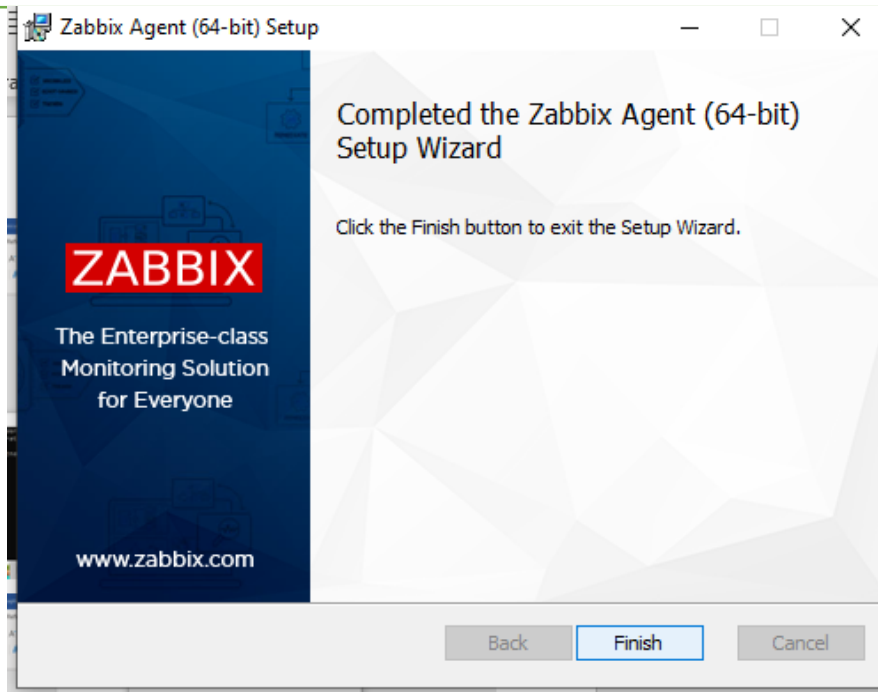


Imagen 162 Agente Zabbix instalado en Windows. [Fuente Propia]

Paso 3: Monitorear

Agregar las plantillas y agentes para monitorear (Plantillas Zabbix)

Las funciones como prueba para demostrar la funcionalidad de la instalación de agentes en ordenadores Windows y monitoreo por Zabbix, mencionando algunos, son las siguientes:

Interfaz ethernet

Interfaz wifi

CPU user time

CPU utilización

CPU Jumps

Memoria utilizada

Todas estas características son parte por defecto de una plantilla de zabbix. Retomando el concepto y el uso de los componentes, una plantilla se compone de ítems y triggers, los ítems recolectan la información de los agentes instalados en ordenadores y los triggers las advertencias.

Se selecciono el ordenador y se ingresó en configuración:

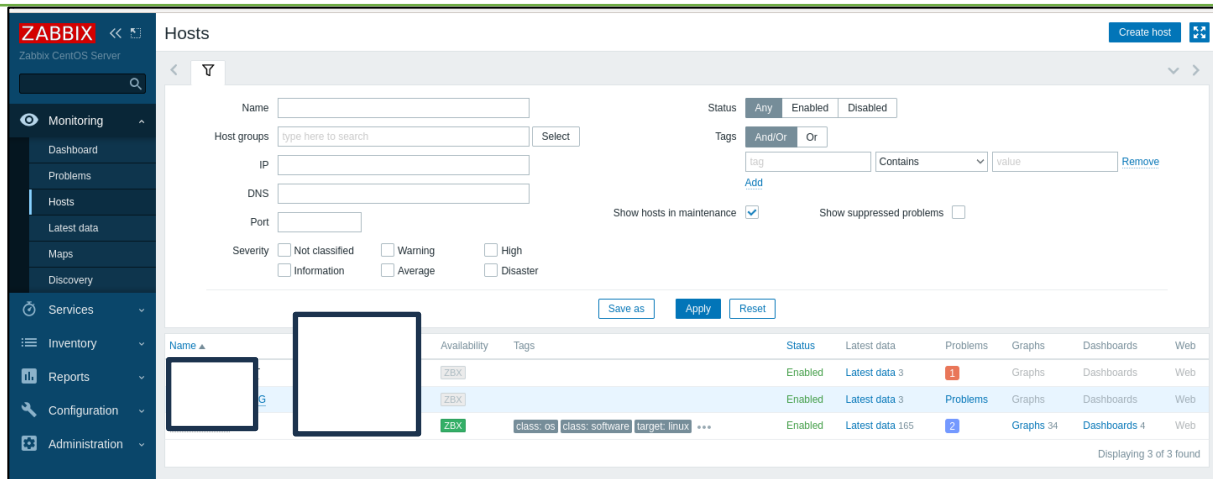


Imagen 163 Selección de ordenador. [Fuente Propia]

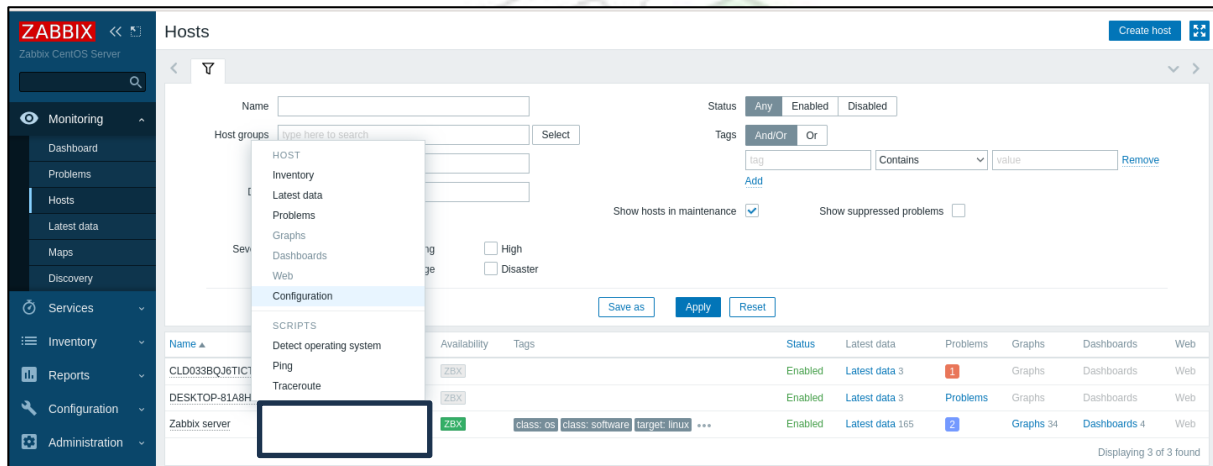


Imagen 164 Selección de configuración. [Fuente Propia]

Agregar la plantilla (Templates)

Se presiona Select en el campo Templates para elegir las platillas. Se elige la plantilla Windows by Zabbix agent, para monitorear el tráfico en el puerto ethernet. El hostGroup de la plantilla es Template:

Hosts

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name

Visible name

Templates Name Action

ICMP Ping Unlink Unlink and clear

type here to search Select

* Groups Select

type here to search

Interfaces Type IP address DNS name Connect to Port Default

Agent IP

Add

Description

Hostboard by name:

Update Clone Full clone Delete Cancel

Imagen 165 Selección de botón template select para elegir plantilla. [Fuente Propia]

Templates

Host group Select

☐ Name

☐ AIX by Zabbix agent

☐ Alcatel Timetra TIMOS by SNMP

☐ Apache ActiveMQ by JMX

☐ Apache by HTTP

☐ Apache by Zabbix agent

☐ Apache Cassandra by JMX

☐ Apache Kafka by JMX

☐ Apache Tomcat by JMX

☐ APC Smart-UPS 2200 RM by SNMP

☐ APC Smart-UPS 3000 XLM by SNMP

☐ APC Smart-UPS RT 1000 RM XL by SNMP

☐ APC Smart-UPS RT 1000 XL by SNMP

☐ APC Smart-UPS SRT 5000 by SNMP

☐ APC Smart-UPS SRT 8000 by SNMP

☐ APC UPS by SNMP

Select Cancel

Imagen 166 Selección de plantilla host group template. [Fuente Propia]

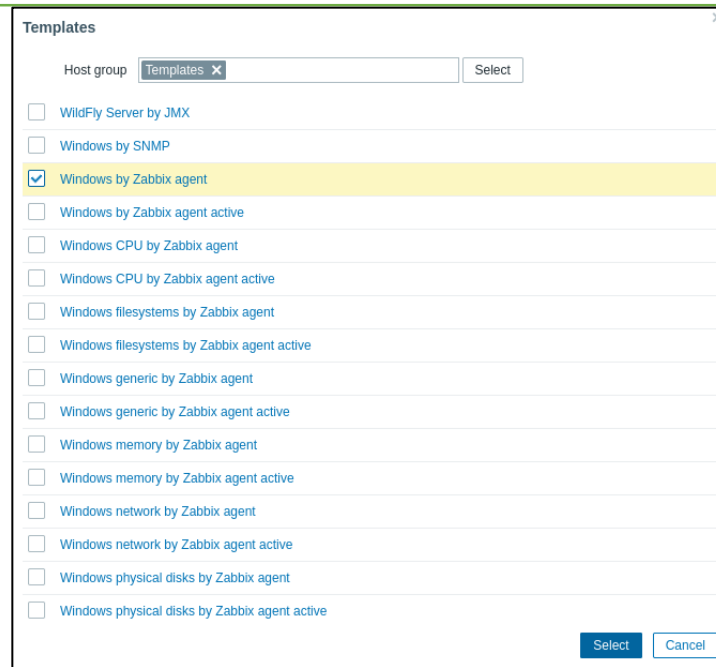


Imagen 167 Selección de Windows by Zabbix Agente template. [Fuente Propia]

Agregar un agente

En el labbel Add, se seleccionó la opción agent y se colocó la dirección IPv4 de el cliente

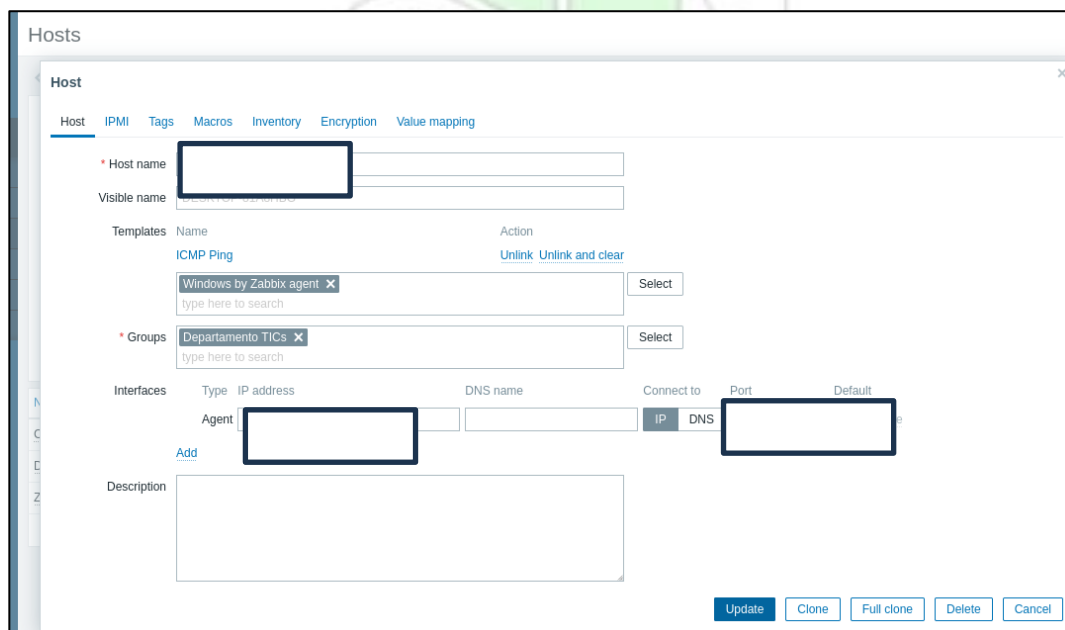


Imagen 168 Agregar un agente para la plantilla seleccionada. [Fuente Propia]

Se añadió haciendo click en el botón update.

Monitoreo

Para monitorear en el menú izquierdo se ingresó en Monitoring, después en Hosts y el nombre del ordenador a monitorear. Se muestra una lista de opciones sobre el host:

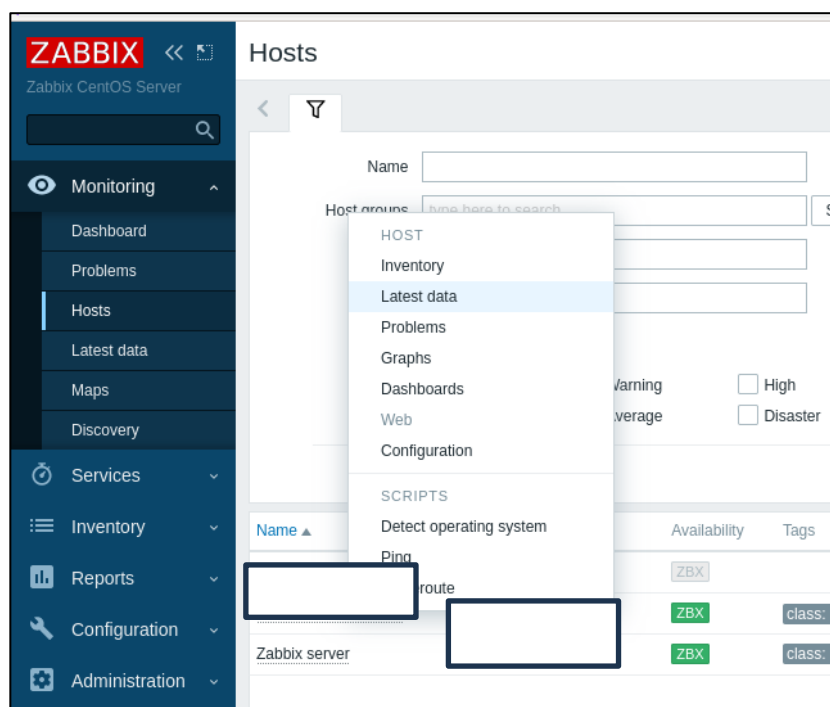


Imagen 169 Latest data del servidor de prueba para ver los datos recolectados. [Fuente Propia]

Al entrar a la opción Latest data se apreció todos los elementos que son monitoreables con la plantilla agregada y enlistados al inicio de este paso No. 3:

Host	Name	Last check	Last value	Change	Tags	Info
	ICMP: ICMP loss	15s	0 %		component: health component: network	Graph
	ICMP: ICMP ping	15s	Up (1)		component: health component: network	Graph
	ICMP: ICMP response time	15s	0.73ms	-0.21ms	component: health component: network	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...	1m 15s	0 bps		component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...	1m 9s	0 bps		component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...	1m 19s	0		component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...	1m 17s	0		component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...				component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...	1m 13s	0		component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...	1m 11s	0		component: network description: WiFi 2 interface: Qualcomm ...	Graph
	Interface Qualcomm Atheros AR9485 Wireless ...				component: network description: WiFi 2 interface: Qualcomm ...	Graph

Imagen 170 Latest data del servidor de prueba para ver los datos recolectados imagen 2. [Fuente Propia]

Name	Unit	Value	Change	Component	Link
Interface Realtek PCIe GbE Family Controller #2...				component: network	Graph
Interface Realtek PCIe GbE Family Controller #2...				component: network	Graph
Interface Realtek PCIe GbE Family Controller #2...	1m 9s	0		component: network	Graph
Interface Realtek PCIe GbE Family Controller #2...	1m 7s	0		component: network	Graph
Interface Realtek PCIe GbE Family Controller #2...				component: network	Graph
Windows: Cache bytes	9s	153.45 MB	-1.75 MB	component: memory	Graph
Windows: Context switches per second	59s	480.5068	+64.8234	component: cpu	Graph
Windows: CPU DPC time	3s	0 %		component: cpu	Graph
Windows: CPU interrupt time	2s	0 %		component: cpu	Graph
Windows: CPU privileged time	1s	4.6154 %	+2.3077 %	component: cpu	Graph
Windows: CPU queue length	58s	2		component: cpu	Graph
Windows: CPU user time	0	0.7692 %	-3.0769 %	component: cpu	Graph
Windows: CPU utilization	55s	8.1131 %	+3.8587 %	component: cpu	Graph
Windows: Free swap space	51s	1.74 GB	+384 KB	component: memory	Graph
Windows: Free swap space in %	4s	96.0182 %	+0.006735 %	component: memory	Graph
Windows: Free system page table entries	8s	12450342	-41	component: memory	Graph
Windows: Host name of Zabbix agent running				component: system	History
Windows: Memory page faults per second	7s	36.4307	+15.7546	component: memory	Graph
Windows: Memory pages per second	6s	0		component: memory	Graph
Windows: Memory pool non-paged	5s	128.75 MB		component: memory	Graph
Windows: Memory utilization	45s	55.6636 %	+0.07024 %	component: memory	Graph
Windows: Network interfaces WMI get				component: raw	

Imagen 171 Latest data del servidor de prueba para ver los datos recolectados imagen 3. [Fuente Propia]

Se apreciaron los valores graficados, tanto individualmente como en conjunto. Obsérvese a continuación las Imágenes sobre algunos ejemplos:

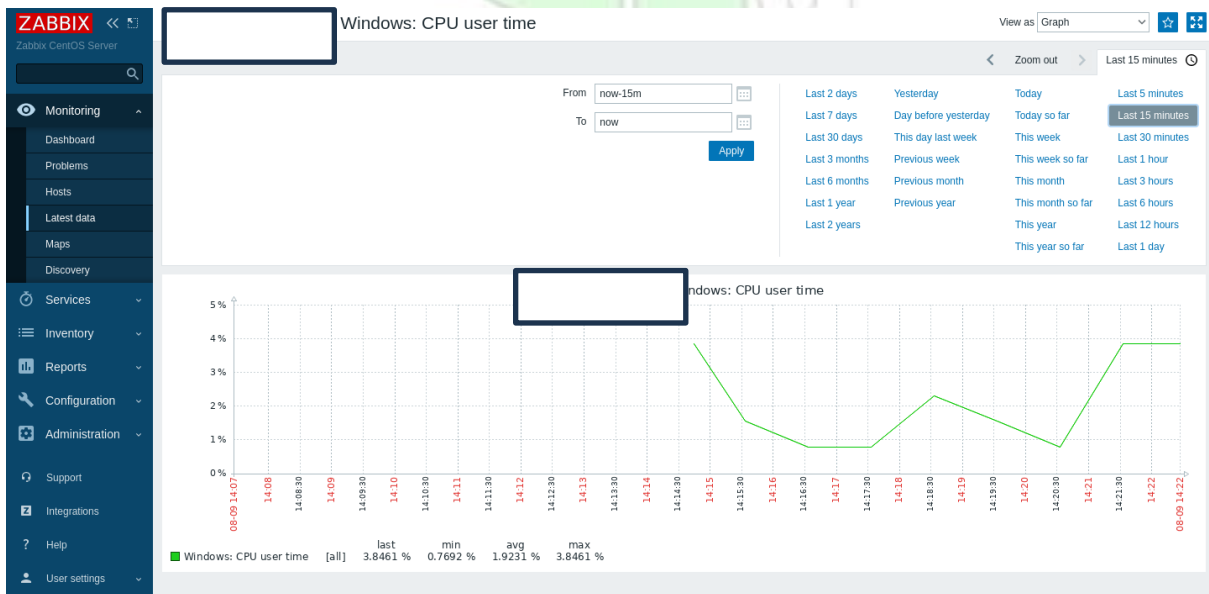


Imagen 172 Gráfica CPU user time de ordenador de prueba. [Fuente Propia]

En la lista de host se seleccionó Graph para visualizar los valores en conjunto

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
		2BX		Enabled	Latest data 3	1	Graphs	Dashboards	Web
		2BX	class: os target: windows	Enabled	Latest data 53	Problems	Graphs 7	Dashboards 2	Web
		2BX	class: os class: software target: linux ***	Enabled	Latest data 165	2	Graphs 34	Dashboards 4	Web

Displaying 3 of 3 found

Imagen 173 Columna Graph de ordenador de prueba. [Fuente Propia]



Imagen 174 Grafica general de CPU usage y CPU utilization de ordenador de prueba. [Fuente Propia]

Se desconecto el ordenador del cable ethernet, entonces las gráficas cambian:

TESCO



Imagen 175 Desconexión de ethernet de ordenador de prueba. [Fuente Propia]

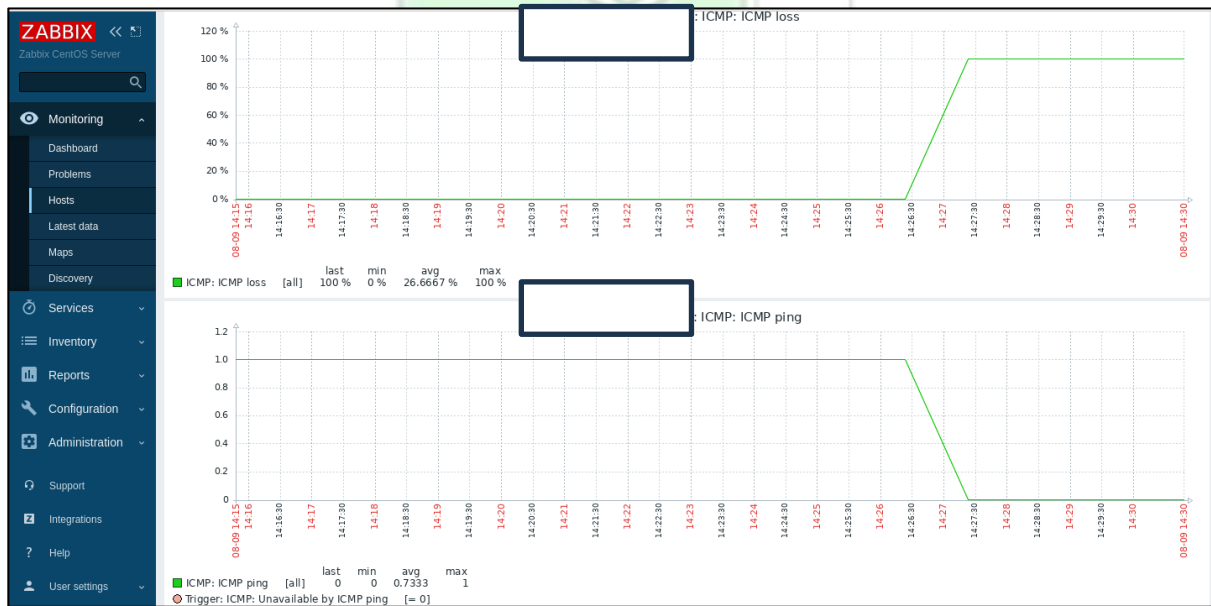


Imagen 176 Cambios en las gráficas de ICMP loss y ping de ordenador de prueba. [Fuente Propia]

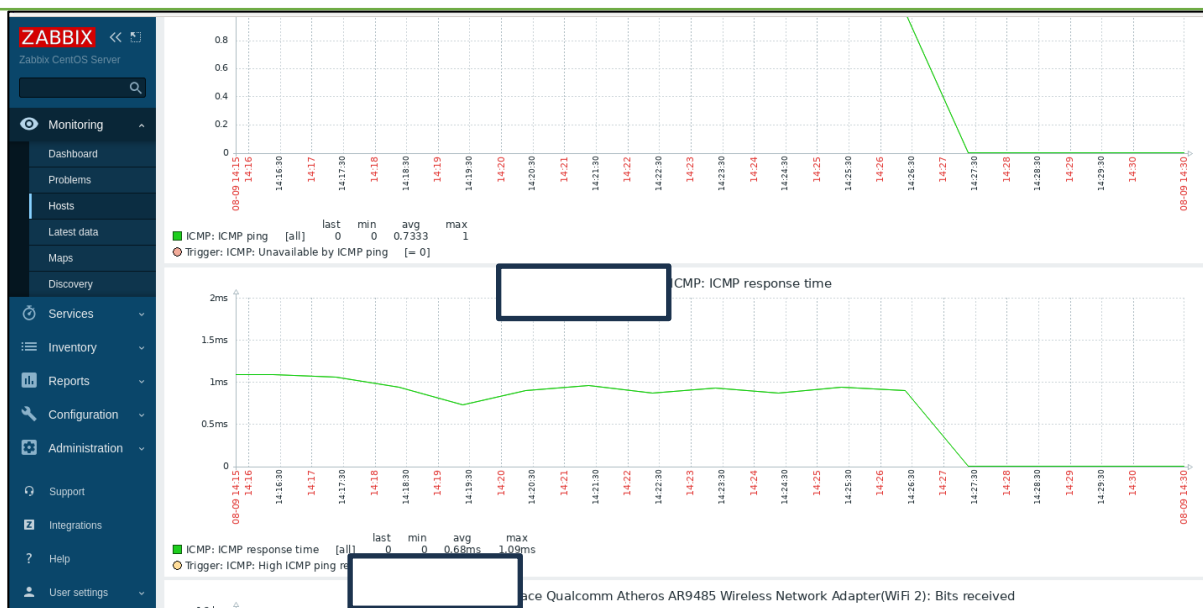


Imagen 177 Cambios en las gráficas de ICMP response time de ordenador de prueba. [Fuente Propia]

Se hizo click en el nombre del host en Monitoring y se ingresó a Problems

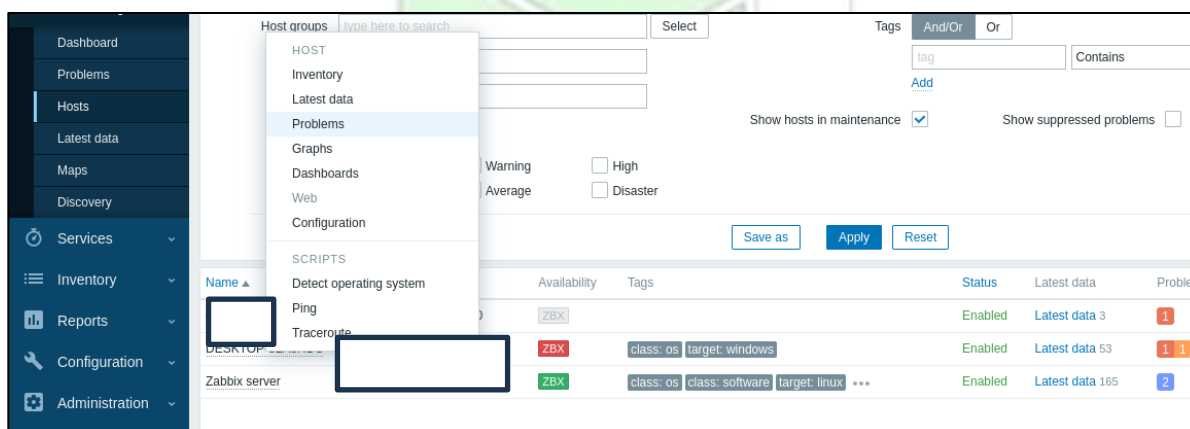


Imagen 178 Opción Problems en ordenador de prueba para visualizar los incidentes. [Fuente Propia]

Aquí se enlistan los problemas o advertencias relacionadas al equipo elegido, el nivel de severidad, la hora, el estado de se encuentra en problemas o está resuelto, que incidente ha sido, entre otros, pero el que a continuación concierte es al presionar No en la columna Ack:

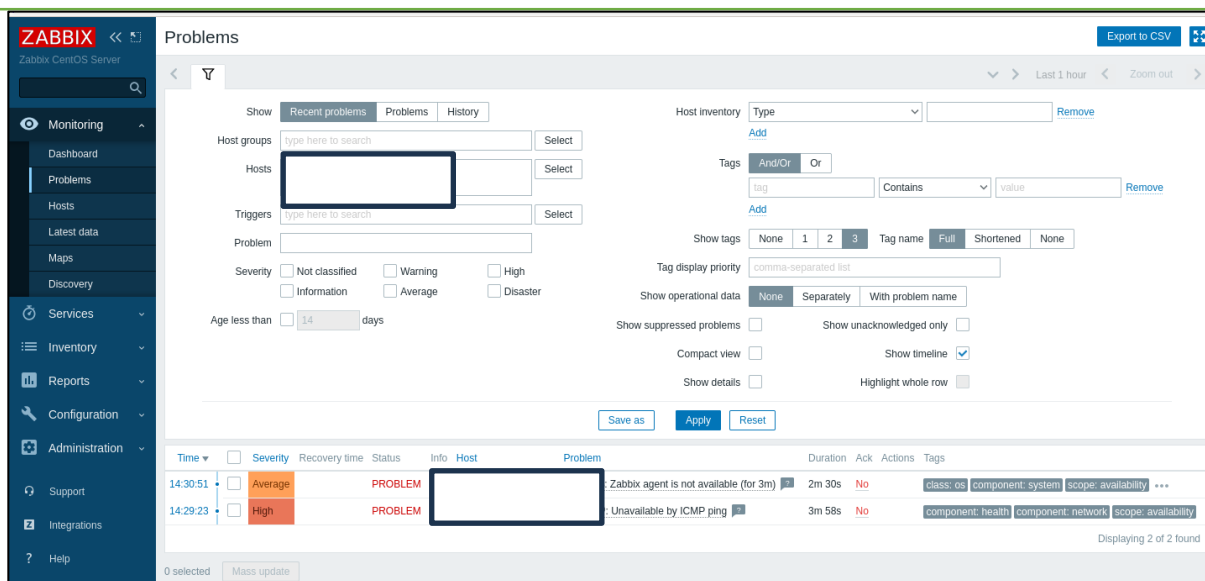


Imagen 179 Problems en ordenador de prueba para visualizar los incidentes. [Fuente Propia]

Se abrió la ventana que permite escribir un mensaje respecto a este problema, modificar el grado de severidad de acuerdo a lo que considere la empresa, si es conocido el incidente y si se desea dar por cerrado:

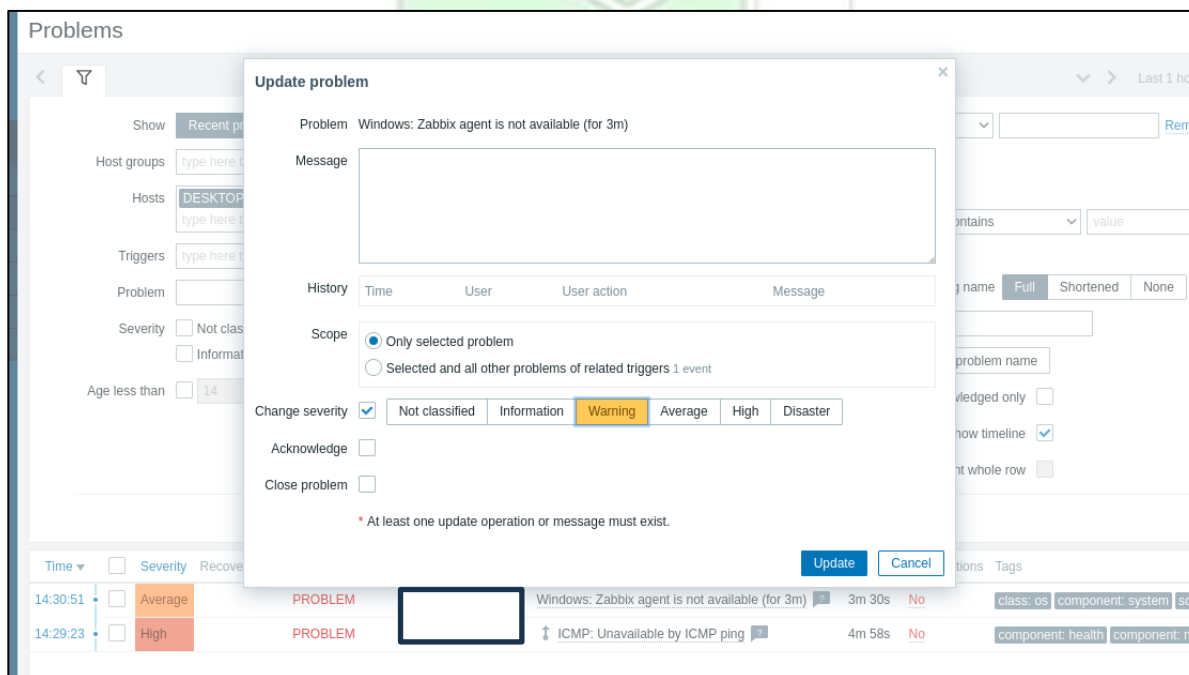


Imagen 180 Ventana de actualización del problema presentado en ordenador de prueba. [Fuente Propia]

Al hacer click en Update, se muestran los cambios:

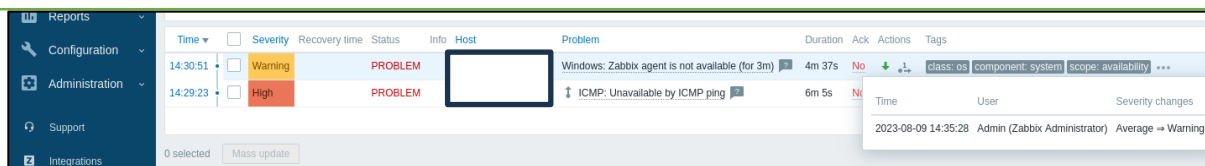


Imagen 181 Cambios realizados al incidente. [Fuente Propia]

Aún lado, en el icono de dialogo, al presionarlo abre información breve de la causa del problema:

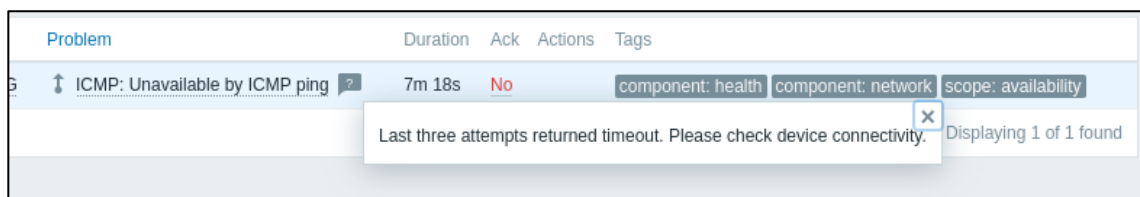


Imagen 182 Información sobre el incidente de ordenador prueba. [Fuente Propia]

Se reconecto el cable ethernet y surgieron nuevamente los cambios en recolección de datos:

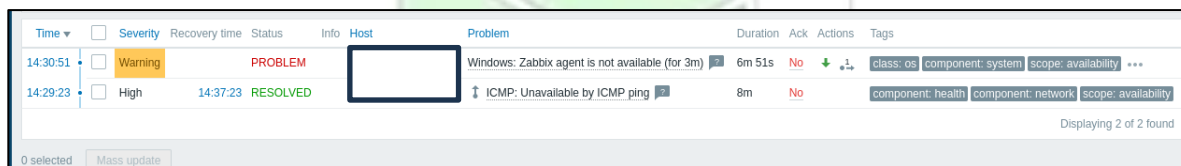


Imagen 183 Resolución de un incidente después de la reconexión de ethernet en ordenador de prueba. [Fuente Propia]

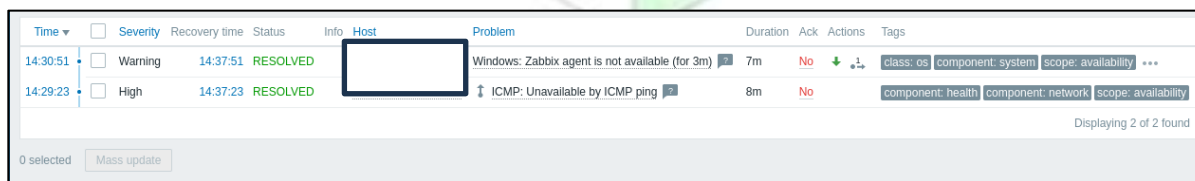


Imagen 184 Resolución de todos los incidentes después de la reconexión de ethernet en ordenador de prueba. [Fuente Propia]

Advertencia de incidentes vía correo electrónico

Se recomienda se debería dedicarse un correo electrónico, o en caso de ya contarlo, incluso si es del mismo jefe de departamento de TICs según sus políticas y procesos tengan en CFE zona Cuautitlán, para recibir correos electrónicos de advertencia si u incidente de seguridad se presentase.

Para hacer uso de este tipo de trigger se deben realizaron los siguientes pasos:

Ingresar a Administrar mi cuenta

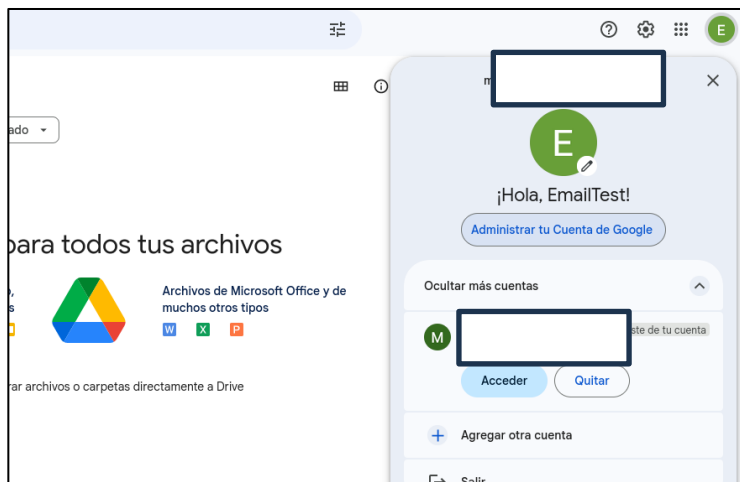


Imagen 185 Opción de administrar mi cuenta de Google. [Fuente Propia]

Dirigirse a seguridad y configurar la verificación de dos pasos

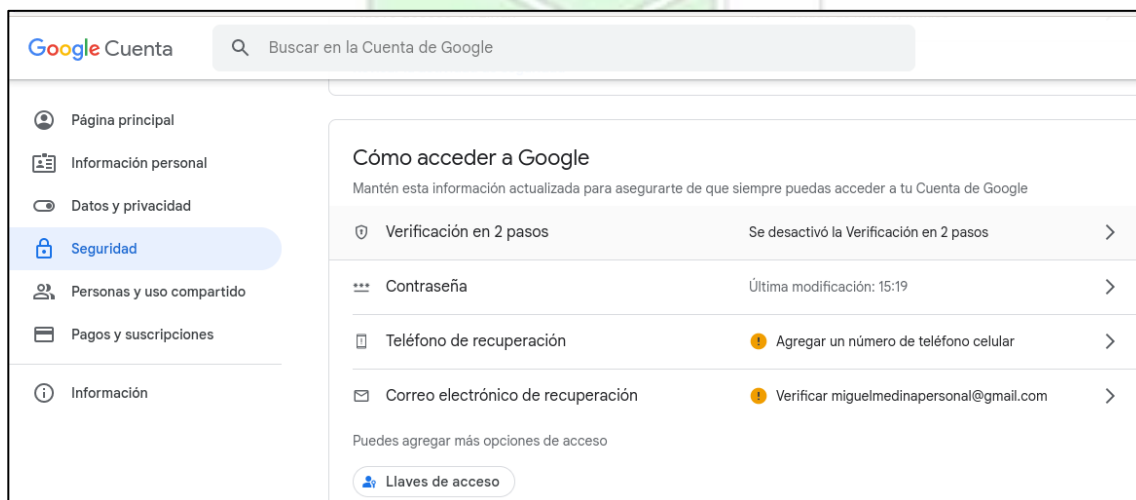


Imagen 186 Opción de verificación en 2 pasos. [Fuente Propia]

← Verificación en 2 pasos

Configurar tu teléfono

¿Qué número de teléfono deseas usar?



Google solo usará este número como método de seguridad de la cuenta.
No ingreses un número de Google Voice.
Se pueden aplicar cargos por mensajes y datos.

¿Cómo deseas obtener los códigos?

☒ Mensaje de texto ☐ Llamada telefónica

[Mostrar más opciones](#)

Paso 1 de 3 [SIGUIENTE](#)

Imagen 187 Llenado de información necesario de verificación en 2 pasos. [Fuente Propia]

Crear una contraseña de aplicaciones:

← Verificación en 2 pasos

Dispositivos que no necesitan un segundo paso

Puedes omitir el segundo paso en los dispositivos de confianza, como en tu propia computadora.

 **Dispositivos de confianza**
Revoca el estado de confianza para tus dispositivos que omitan la verificación en 2 pasos.

[REVOCAR TODOS](#)

Contraseñas de aplicaciones

No se recomienda usar contraseñas de la aplicación y estas son innecesarias en la mayoría de los casos. A fin de proteger tu cuenta, usa "Acceder con Google" para conectar apps a tu Cuenta de Google.

Contraseñas de aplicaciones
Ninguna [>](#)

Imagen 188 Creación de una contraseña para aplicaciones. [Fuente Propia]

Para Zabbix se colocó en la opción de Otros en aplicaciones. El nombre de la aplicación es personalizado:



← **Contraseñas de aplicaciones**

La Contraseña de la aplicación te permite acceder a tu cuenta de Google desde apps en dispositivos que no son compatibles con la verificación en 2 pasos. Solo debes ingresarla una vez para que no tengas que recordarla. [Más información](#)

No tienes contraseñas de la aplicación.

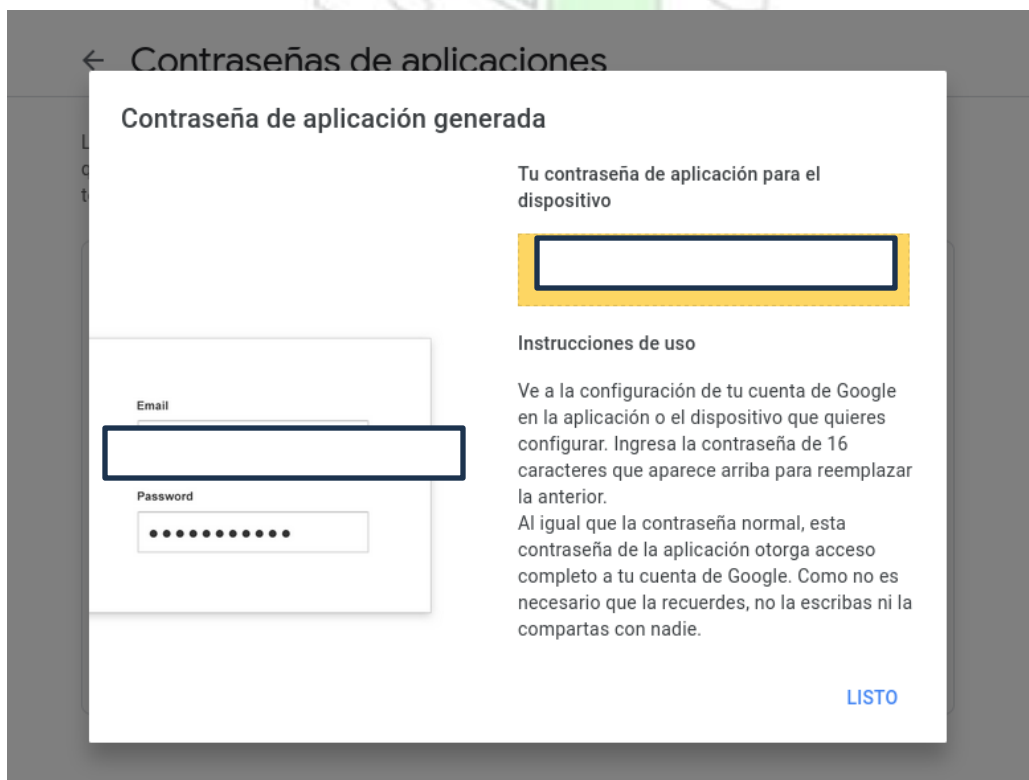
Selecciona la app y el dispositivo para los que quieras generar la Contraseña de la aplicación.

X

GENERAR

Imagen 189 Creación de una contraseña para Zabbix. [Fuente Propia]

Se genero la contraseña para que Gmail permita a Zabbix la entrada de sus correos electrónicos. Esta contraseña solo se muestra una vez por lo que debe anotarse:



← **Contraseñas de aplicaciones**

Contraseña de aplicación generada

Tu contraseña de aplicación para el dispositivo

Instrucciones de uso

Ve a la configuración de tu cuenta de Google en la aplicación o el dispositivo que quieres configurar. Ingresa la contraseña de 16 caracteres que aparece arriba para reemplazar la anterior.

Al igual que la contraseña normal, esta contraseña de la aplicación otorga acceso completo a tu cuenta de Google. Como no es necesario que la recuerdes, no la escribas ni la compartas con nadie.

LISTO

Email

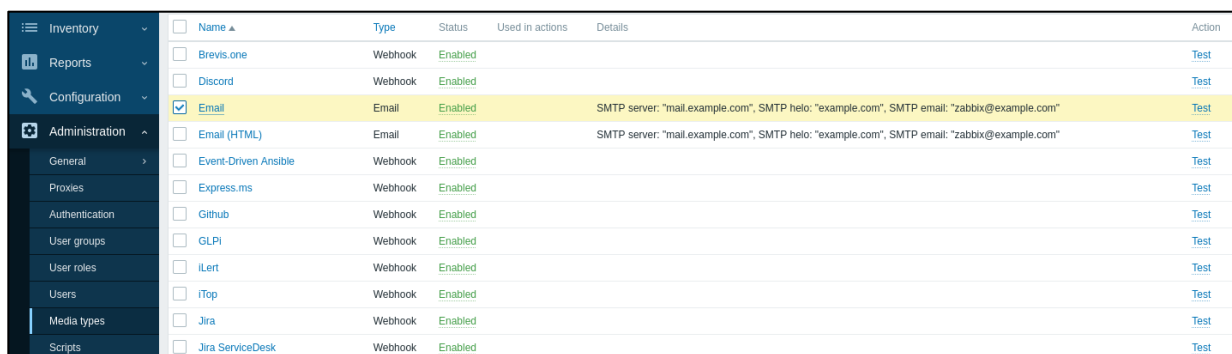
Password

Imagen 190 Contraseña generada para el envío de correos por Zabbix. [Fuente Propia]

Ahora para la demostración del envío de correo electrónico de advertencia, se desconectó el ordenador de prueba del switch donde se encuentra el servidor y dejar que envíe Zabbix un correo Gmail.

Antes de esto se debe configurar lo siguiente en Zabbix:

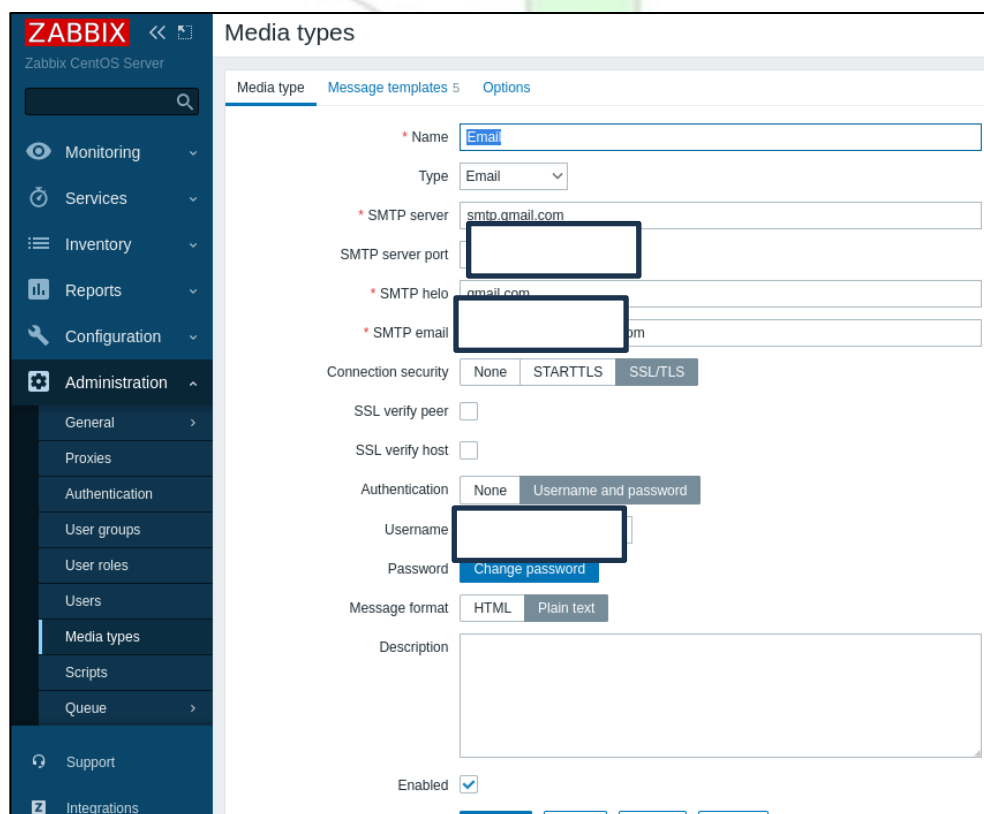
Entrar a Administration > Media Types y presionar en el nombre con azul que dice Email.



Name	Type	Status	Used in actions	Details	Action
Brevis.one	Webhook	Enabled			Test
Discord	Webhook	Enabled			Test
Email	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	Test
Email (HTML)	Email	Enabled		SMTP server: "mail.example.com", SMTP helo: "example.com", SMTP email: "zabbix@example.com"	Test
Event-Driven Ansible	Webhook	Enabled			Test
Express.ms	Webhook	Enabled			Test
Github	Webhook	Enabled			Test
GLPI	Webhook	Enabled			Test
ILert	Webhook	Enabled			Test
ITop	Webhook	Enabled			Test
Jira	Webhook	Enabled			Test
Jira ServiceDesk	Webhook	Enabled			Test

Imagen 191 Configuración de email en zabbix. [Fuente Propia]

Configurar con los siguientes valores:



ZABBIX << Zabbix CentOS Server

Media types

Media type Message templates 5 Options

Name

Type

SMTP server

SMTP server port

SMTP helo

SMTP email

Connection security ☐ ☐ ☒

SSL verify peer ☐

SSL verify host ☐

Authentication ☐ ☒

Username

Password

Message format ☐ ☐

Description

Enabled ☒

Imagen 192 Configuración de email en zabbix en media types. [Fuente Propia]

Ahora Configuration > Actions > Trigger Actions,

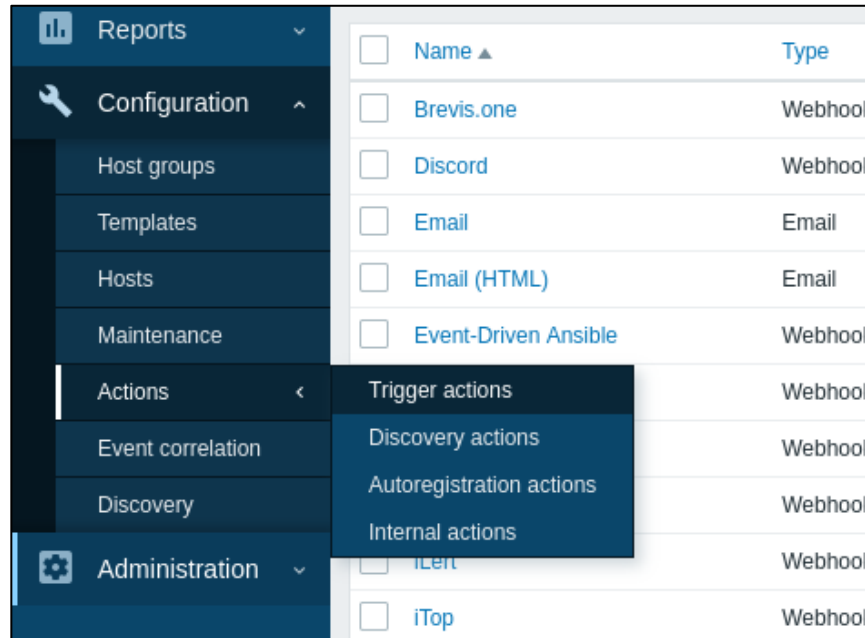


Imagen 193 Configuración de acciones de triggers en Configuration. [Fuente Propia]

Click en Add en Conditions, seleccionar Type, el tipo de trigger siendo en este caso Trigger severity, el operador lógico y a que grado de severidad un evento deberá notificarse:

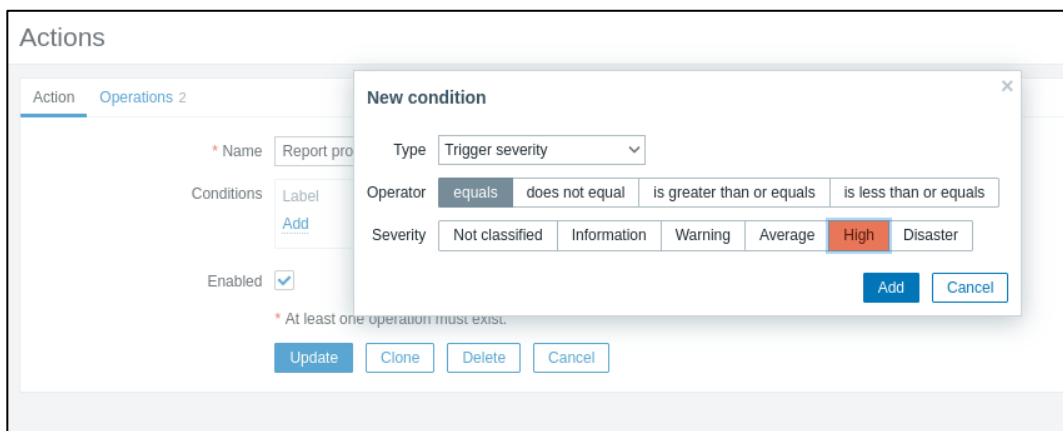


Imagen 194 Configuración de acciones de triggers en new conditions. [Fuente Propia]

En la pestaña Operations se ingresó la siguiente configuración:

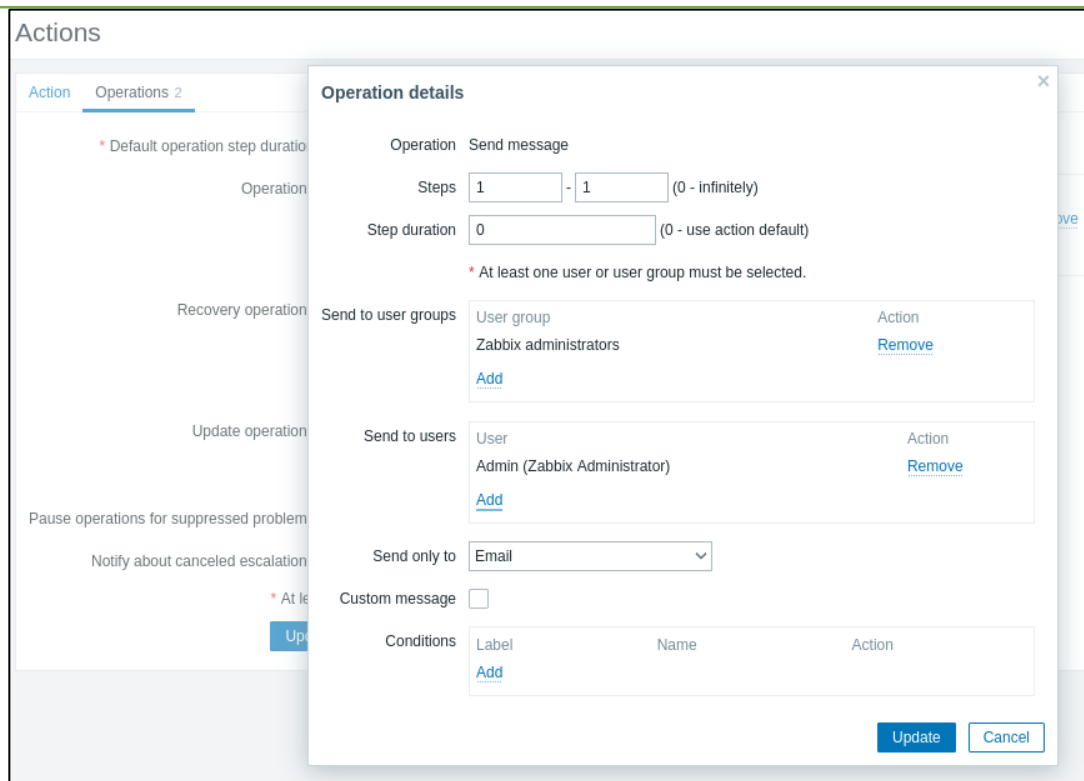


Imagen 195 Configuración de acciones de triggers en Operation details. [Fuente Propia]

Entrar a User Setting > Profile, asegurarse que el tiempo de zona horaria sea correcto.

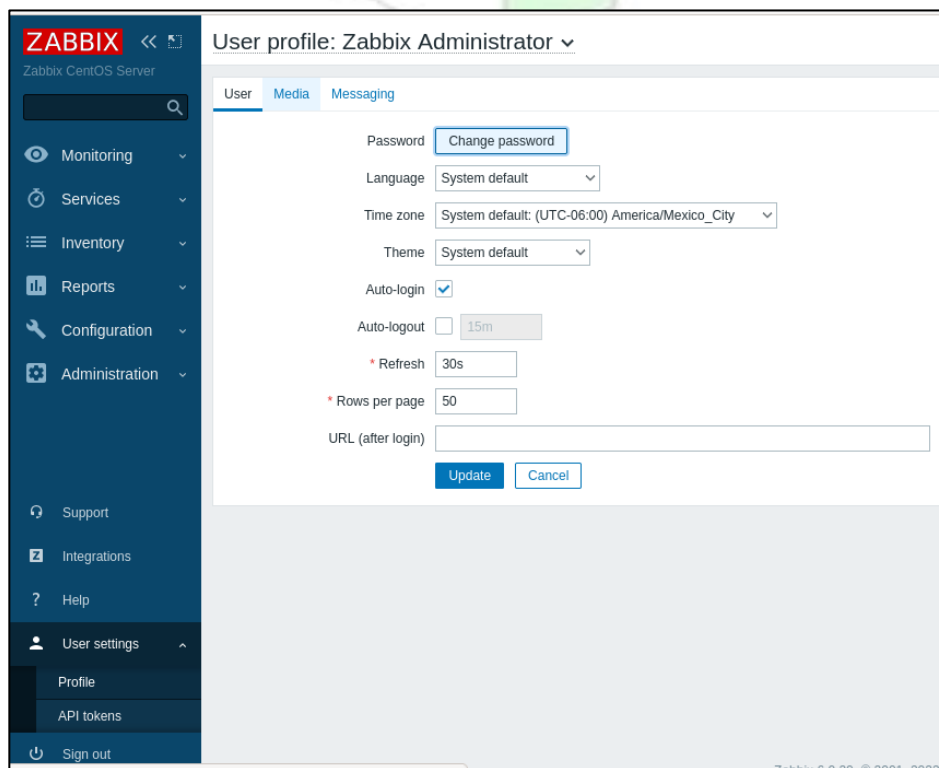


Imagen 196 Configuración de user profile del administrador del usuario zabbix. [Fuente Propia]

Ingresar a Media, añadir el Gmail y habilitarlo

User profile: Zabbix Administrator ▾

User Media 1 Messaging

Media	Type	Send to	When active	Use if severity	Status	Action
	Email	[Redacted]	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove

Add Update Cancel

Imagen 197 Configuración de user profile del administrador del usuario zabbix en pestaña Media. [Fuente Propia]

Se envió un mensaje de prueba:

Test media type "Email" ✕

✓ Media type test successful. ✕

* Send to [Redacted]@mail.com

Subject Test subject

* Message This is the test message from Zabbix

Test Cancel

Imagen 198 Envío de prueba de correo electrónico de advertencia de evento de Zabbix. [Fuente Propia]

Al desconectar el equipo del puerto ethernet, observamos en la información de actions que en Zabbix ya se cuenta con este tipo de trigger implementado:

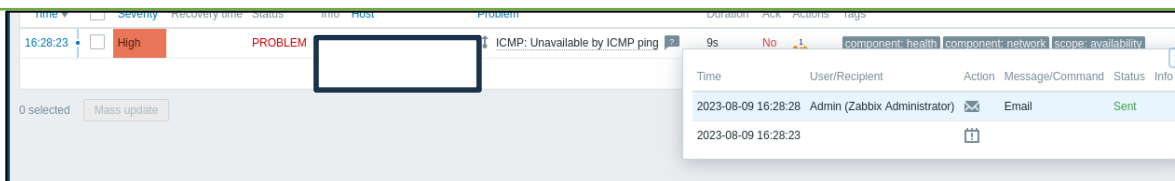


Imagen 199 Email conImagendo y desplegado en acciones de un problema en zabbix. [Fuente Propia]

En el correo electrónico al instante que zabbix detecta el problema y la severidad, envía el mensaje de advertencia:

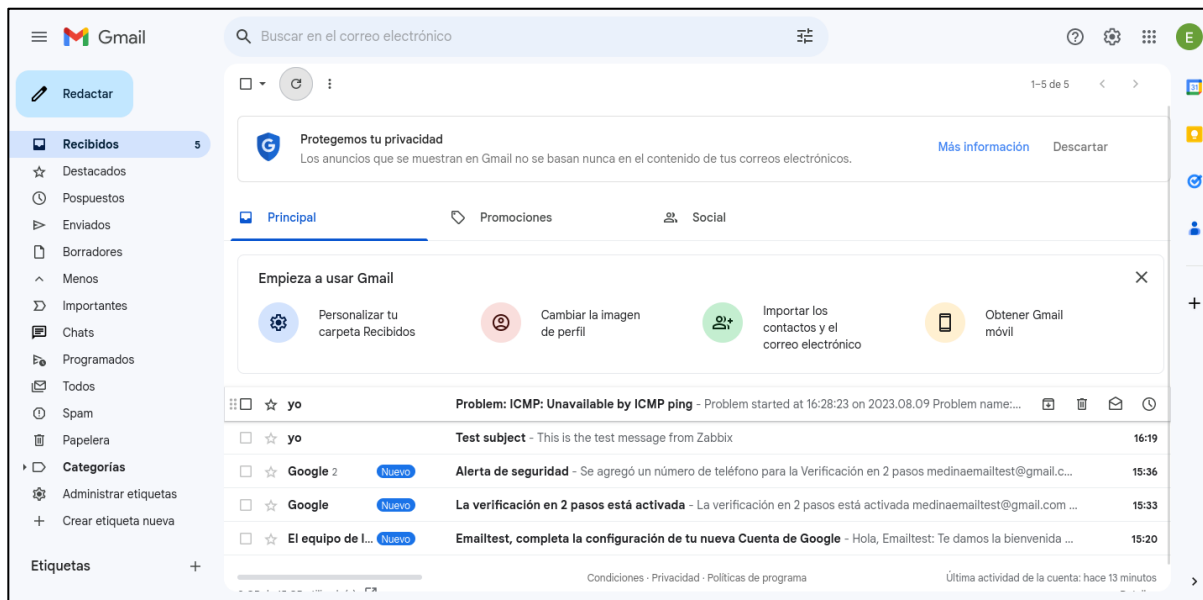


Imagen 200 Correo de prueba y de notificación de error en Gmail. [Fuente Propia]

Por lo que se observa la indicación de problemas es un proceso automatizado, y facilita la interpretación de Zabbix o como una alarma en caso de que el jefe de departamento no se encuentre en la zona de labores. Además de que no solo puede advertir a un usuario o una sola dirección de correo electrónico, puede avisar a otros miembros siempre y cuando por reglas de seguridad, tengan autorización para conocer del asunto.

Así como estos aspectos monitoreables y el tipo de trigger anterior, Zabbix es una herramienta aún más escalable y adaptable.

CONCLUSIONES

Es importante abordar los problemas y desafíos de las empresas mediante la colaboración de personas con experiencia tanto interna como externa. En el caso específico de la entidad CFE en la zona Cuautitlán, se llevaron a cabo análisis utilizando diversos enfoques, como cuestionarios, análisis FODA, evaluación de riesgos y referencia a la norma ISO-IEC 27001:2013. Estos análisis identificaron vulnerabilidades de distintos niveles de riesgo, enfocándose en aspectos como posibles ataques informáticos y la escasez de personal en el departamento de TIC.

Para abordar estas vulnerabilidades, se propusieron estrategias y recomendaciones basadas en estándares reconocidos, como la norma ISO-IEC 27001:2013 y el marco de trabajo COBIT 4.0. Entre estas estrategias, se destacó la investigación y la implementación de un servidor en CentOS para la herramienta de monitoreo Zabbix para la intranet de CFE en zona Cuautitlán, con el propósito de fortalecer el control y la seguridad de la red.

La implementación del servidor se basó en investigaciones de fuentes originales y confiables como CentOS y Red Hat, y se realizaron pruebas tanto de instalación como de uso de Zabbix, asegurando que se cumplieran los requisitos y se lograra el propósito deseado. Es así como uno de los principales protocolos, el ICMP cumplió con los requisitos al funcionar con una herramienta de software gratuita y al cumplir su función de monitoreo de disponibilidad y latencia de la red.

La herramienta Zabbix se destaca como una solución viable a pesar de su licencia gratuita, igualmente en otro punto en sistemas Windows para recopilar información del sistema y del hardware, se ha determinado como recomendación la implementación de agentes de Zabbix evitando con ello las complejidades y vulnerabilidades asociadas con el protocolo SNMP.

Zabbix contribuye a la detección de anomalías a través de sus "triggers", alertando a los usuarios con acceso y configuración adecuados en la base de datos y el servidor, con configuraciones definidas por el administrador. Finalmente, la empresa debe siempre mantener un enfoque estratégico, preventivo y proactivo en la seguridad de la información, basado en estándares reconocidos y herramientas efectivas, con o sin licencia siempre y cuando provengan de fuentes seguras y expertas en el área de seguridad para mejorar el rendimiento de la red y de sus departamentos, por ende, de sus servicios y calidad.

Como recomendación para implementaciones futuras, la empresa debe invertir o asignar un presupuesto adecuado sustentado por los análisis resultantes de este reporte así como análisis llevados a cabo por la misma empresa para la mejora del monitoreo en la red además de tratar otros problemas dentro del Departamento de Tecnologías de la Información, sea como ejemplo la adquisición de licencia de un software de monitoreo que tenga una amplia gama de herramientas, interfaces y protocolos de monitoreo de redes.

Gracias a este proyecto y la oportunidad de realizarlo he aprendido a aplicar técnicas de recolección de datos, realizar con la información obtenida y con la norma ISO-IEC 27001:2013 métricas de evaluación o de relación entre datos. Así mismo a integrar el conocimiento obtenido con herramientas de software para monitorear dispositivos finales en una intranet.



TESCO

COMPETENCIAS DESARROLLADAS

Durante el desarrollo y finalización del presente proyecto para la Comisión Federal de Electricidad las competencias en las que más destaque e implemente fueron:

ASIGNATURA	COMPETENCIA
Auditoría Informática de Desarrollo de Proyectos y Aplicaciones	1) Identifica, interpreta y usa de lineamientos, estándares, marcos referenciales, técnicas y otros conceptos que complementen la unión del conocimiento para la posterior aplicación de la Auditoría informática. 2) Describe las herramientas aplicables a la Auditoría, a fin de proponerlas en el desarrollo de la planificación, ejecución y entrega de resultados del proceso de auditoría informática. 3) Comprende el entorno del control interno en las empresas y su concepción en una normativa internacional
Administración de la Función Informática	Utiliza funciones de la administración orientadas a la seguridad para la realización de planes que le permitan responder ante incidentes de seguridad.
Administración de Redes	1) Instala, configura y administra diferentes servicios de red para satisfacer las necesidades específicas de las organizaciones. 2) Analiza y monitorea la red para medir su

	desempeño y fiabilidad con herramientas de software.
Redes de Computadoras	Selecciona y configura los dispositivos adecuados para garantizar el funcionamiento correcto de una red local.
Ingeniería de Software	Abstrae información del usuario final para elaborar el análisis de requerimientos del software a desarrollar.
Taller de Investigación II	1) Analiza y conforma la actualización del protocolo de investigación para darle seguimiento. 2) Realiza el proyecto de investigación ante diversos escenarios con actitud crítica y constructiva para la solución de problemas relacionados con su campo profesional.

Estas competencias las he empleado en la implementación de la herramienta de software Zabbix, herramienta con aplicaciones escalables, para solucionar posibles incidentes en la red por parte de los ordenadores de los usuarios, en un entorno de servidor con sistema CentOS y clientes con sistemas Windows, donde por parte del servidor se integran otras herramientas de software como la instalación PHP, MySQL y Apache server.

Se evaluó los requerimientos de software y hardware mínimos necesarios para zabbix y los que fueron finalmente proporcionados por la empresa, con ellos una serie de instrucciones de la instalación del software.

Se detectaron áreas de oportunidad en el departamento de TIC's basado en cuestionarios, análisis de riesgos y FODA's basados en la norma ISO-IEC 27001:2013, recomendaciones y estrategias involucrando al jefe de departamento de TIC's y a la autoridad correspondiente, sugiriendo acciones preventivas y correctivas, tanto de origen informativa como tecnológica.

FUENTES DE INFORMACIÓN

APA. (s.f.). APA. American Psychological Association:
style.apa.org

arlethv. (11 de abril de 2022). Capa 3 vs Capa 2. HUAWEI:
forum.huawei.com/enterprise/es/Capa-3-vs-Capa-2/thread/667233959152599041-667212890693840896

CentOS. (s.f.). About CentOS. CentOS.org:
centos.org/about/

CentOS. (s.f.). Comparing CentOS Stream and CentOS Linux. CentOS.org:
centos.org/cl-vs-cs/

Ceruzzi, P. E. (2017). A History of Modern Computing. MIT Press.

CFE. (s.f.). ¿Qué es la CFE?. Comisión Federal de Electricidad:
cfe.mx/nuestraempresa/pages/queeslacfe.aspx

CISCO. (s.f.). What Is Network Address Translation (NAT)?. CISCO:
cisco.com/c/en/us/products/routers/network-address-translation.html

CloudFlare. (s.f.). What is the Internet Control Message Protocol (ICMP)?:
cloudflare.com/en-gb/learning/ddos/glossary/internet-control-message-protocol-icmp/

Diana M. (junio de 2009). Metodología para el establecimiento de objetivos de control como un medio de seguridad en el área de tecnologías de información:
tesis.ipn.mx/handle/123456789/6771

Freeman, J., & Freeman, E. (2015). Cloud Computing: Concepts, Technology & Architecture. Prentice Hall.

Gromala, D., & Vogan, D. (Eds.). (2019). Stories of Software: From Abstract to Practical. MIT

Press.

ISACA. (2005). Cobit 4.0. Gobierno de México:

gob.mx/cms/uploads/attachment/file/82967/CobiT4_Espanol.pdf

José Talledo San Miguel. (s.f.). Implantación de aplicaciones web en entornos internet, intranet y extranet. Google academico:

books.google.es/books?hl=es&lr=&id=RtESCgAAQBAJ&oi=fnd&pg=PA1&dq=intranet&ots=2hyBdReE6o&sig=0reKAbg2qaDiXDW_YncQH8pSxMw#v=onepage&q=intranet&f=false

Mozilla. (s.f.). Asíncrono:

developer.mozilla.org/es/docs/Glossary/Asynchronous

Oracle. (s.f.). StorageTek Guía de referencia de SNMP para SL150/SL500/SL3000/SL8500:

docs.oracle.com/cd/E24292_01/es/E50682/html/snmpmib.htm

PAESSLER. (s.f.). IT Explained: Servidor:

paessler.com/es/it-explained/server

PAESSLER. (s.f.). Supervisión de sistemas operativos con PRTG:

[paessler.com/es/operating-system-](https://paessler.com/es/operating-system-monitoring#:~:text=¿Qué%20es%20un%20sensor%20en,libre%20de%20un%20disco%20duro.)

[monitoring#:~:text=¿Qué%20es%20un%20sensor%20en,libre%20de%20un%20disco%20duro.](https://paessler.com/es/operating-system-monitoring#:~:text=¿Qué%20es%20un%20sensor%20en,libre%20de%20un%20disco%20duro.)

PAESSLER. (s.f.). TI explained: SNMP:

Paessler.com/es/it-explained/snmp

Red Hat. (03 de enero de 2023). La distribución de Linux más conveniente para usted. Red Hat:

redhat.com/es/topics/linux/whats-the-best-linux-distro-for-you

Red Hat. (03 de Enero de 2023). ¿Qué es CentOS?. Red Hat:

redhat.com/es/topics/linux/what-is-centos

Red Hat. (31 de enero de 2023). ¿Qué es una máquina virtual?. Red Hat:

redhat.com/es/topics/virtualization/what-is-a-virtual-machine

Red Hat. (24 de octubre de 2019). What is open source?. Red Hat:

redhat.com/en/topics/open-source/what-is-open-source

Zabbix. (s.f.). 8 Templates and template groups:

zabbix.com/documentation/current/en/manual/config/templates#:~:text=A%20template%20is%20a%20set,graphs

Zabbix. (s.f.). Documentation Agent:

zabbix.com/documentation/current/es/manual/concepts/agent#:~:text=El%20agente%20Zabbix%20se%20implementa,Zabbix%20para%20su%20posterior%20procesamiento.

Zabbix. (s.f.). Documentación Items. Zabbix:

zabbix.com/documentation/current/es/manual/config/items



TESCO

ANEXOS

A.1 ISO-IEC 27001:2013 Análisis de riesgos, Requisito 6.1.2. Apreciación de riesgos de seguridad de la información, [Fuente Norma Española UNE-ISO/IEC 27001:2013, 2014].

6.1.2 Apreciación de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información que:

- a) establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:
 - 1) los criterios de aceptación de los riesgos, y
 - 2) los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;
- b) asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generen resultados consistentes, válidos y comparables;
- c) identifique los riesgos de seguridad de la información:
 - 1) llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,
 - 2) identificando a los dueños de los riesgos;
- d) analice los riesgos de seguridad de la información:
 - 1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,
 - 2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),
 - 3) determinando los niveles de riesgo;
- e) evalúe los riesgos de seguridad de la información:
 - 1) comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),
 - 2) priorizando el tratamiento de los riesgos analizados.

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

A.2 ISO-IEC 27001:2013 Anexo A.16. Gestión de incidentes de seguridad de la información, [Fuente Norma Española UNE-ISO/IEC 27001:2013, 2014].

A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	<i>Control</i> Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
A.16.1.2	Notificación de los eventos de seguridad de la información	<i>Control</i> Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.
A.16.1.3	Notificación de puntos débiles de la seguridad	<i>Control</i> Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	<i>Control</i> Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	<i>Control</i> Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	<i>Control</i> El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.
A.16.1.7	Recopilación de evidencias	<i>Control</i> La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.

A.3 ISO-IEC 27001:2013 Anexo A.13, Seguridad de las comunicaciones, [Fuente Norma Española UNE-ISO/IEC

A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.		
A.13.1.1	Controles de red	<i>Control</i> Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	<i>Control</i> Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.
A.13.1.3	Segregación en redes	<i>Control</i> Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.
A.13.2 Intercambio de información		
Objetivo: Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de intercambio de información	<i>Control</i> Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.
A.13.2.2	Acuerdos de intercambio de información	<i>Control</i> Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.
A.13.2.3	Mensajería electrónica	<i>Control</i>

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operacionales		
Objetivo: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.		
A.12.1.1	Documentación de procedimientos operacionales	Control Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben ser controlados.
A.12.1.3	Gestión de capacidades	Control Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.
A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	Control Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
A.12.2 Protección contra el software malicioso (malware)		
Objetivo: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.		
A.12.2.1	Controles contra el código malicioso	Control Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.
A.12.3 Copias de seguridad		
Objetivo: Evitar la pérdida de datos		
A.12.3.1	Copias de seguridad de la información	Control Se deben realizar copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.
A.12.4 Registros y supervisión		
Objetivo: Registrar eventos y generar evidencias.		
A.12.4.1	Registro de eventos	Control Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.
A.12.4.2	Protección de la información del registro	Control Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.
A.12.4.3	Registros de administración y operación	Control Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.

A.5 ISO-IEC 27001:2013 Requisito 10.2 Mejora continua, [Fuente Norma Española UNE-ISO/IEC 27001:2013, 2014].

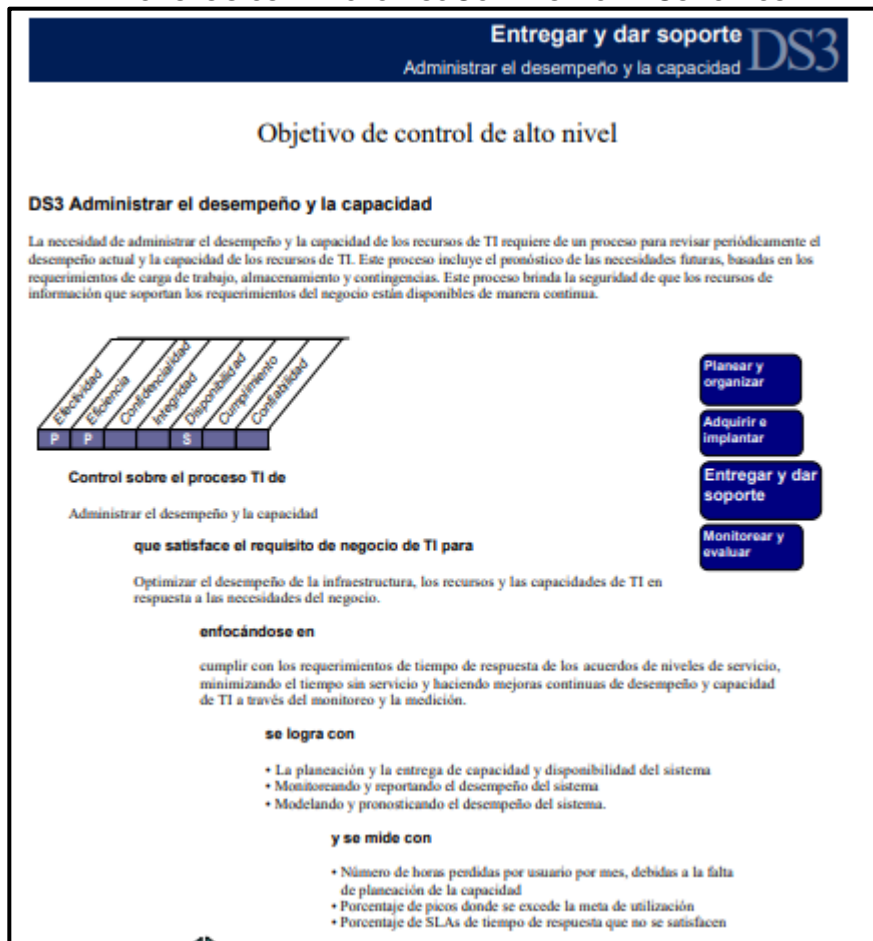
10.2 Mejora continua

La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

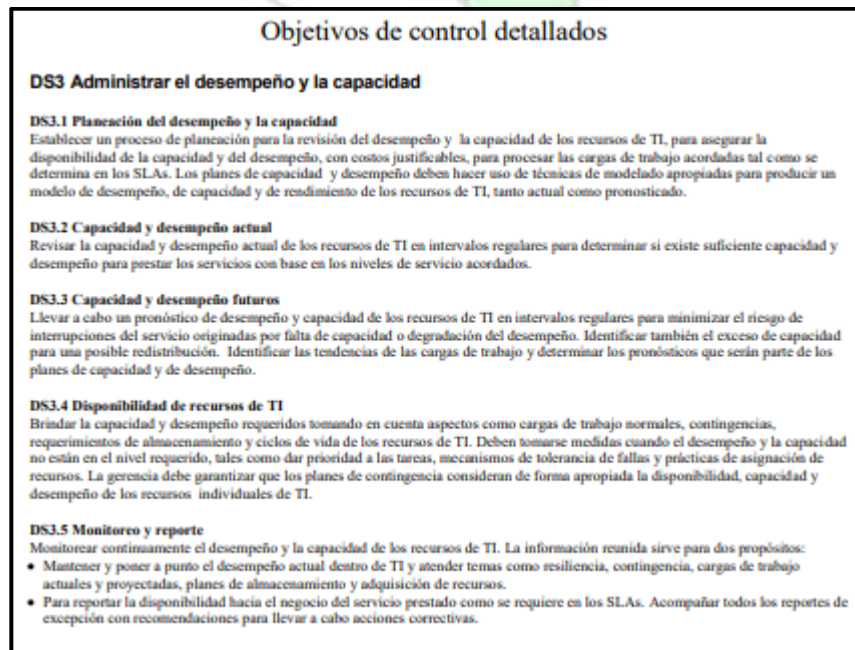
A.6 ISO-IEC 27001:2013 Anexo A.9 Control de acceso, [Fuente Norma Española UNE-ISO/IEC 27001:2013, 2014].

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Limitar el acceso a los recursos de tratamiento de la información y a la información.		
A.9.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de red	Control Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.
A.9.2 Gestión de acceso de usuario		
Objetivo: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuario	Control Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.
A.9.2.2	Provisión de acceso de usuario	Control Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.
A.9.2.3	Gestión de privilegios de acceso	Control La asignación y el uso de privilegios de acceso debe estar restringida y controlada.
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Control La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.
A.9.2.5	Revisión de los derechos de acceso de usuario	Control Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.
A.9.2.6	Retirada o reasignación de los derechos de acceso	Control Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.		
A.9.3.1	Uso de la información secreta de autenticación	Control Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
A.9.4 Control de acceso a sistemas y aplicaciones		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	Control Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.
A.9.4.2	Procedimientos seguros de	Control
	inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.
A.9.4.3	Sistema de gestión de contraseñas	Control Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.
A.9.4.4	Uso de utilidades con privilegios del sistema	Control Se debe restringir y controlar rigurosamente el uso de utilidades que puedan capacitar de invalidar los controles del sistema y de la aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.



B.2 COBIT 4.0 DS3 Administrar el desempeño y la capacidad, Objetivos de control detallados [Fuente COBIT 4.0, 2005].



B.3 COBIT 4.0 DS3 Administrar el desempeño y la capacidad, Directrices Gerenciales, [Fuente COBIT 4.0, 2005].

Directrices Gerenciales

DS3 Administrar el desempeño y la capacidad

Desde	Entradas	Salidas	Para
A2	Especificaciones de disponibilidad, continuidad y de recuperación	Información sobre desempeño y capacidad	PO2 PO3
A3	Requerimientos de monitoreo del sistema	Plan de desempeño y capacidad (requerimientos)	PO5 A11 A13 ME1
DS1	SLAs	Cambios requeridos	A16
		Reportes de desempeño del proceso	ME1

Gráfica RACI

Funciones

Actividades

Establecer un proceso de planeación para la gestión del desempeño y la capacidad de los recursos de TI
 Revisar el desempeño y la capacidad actual de los recursos de TI
 Realizar pronósticos de desempeño y capacidad de los recursos de TI
 Realizar análisis de brecha para identificar incompatibilidad de los recursos de TI
 Realizar un plan de contingencia respecto a una potencial falla de disponibilidad de recursos de TI
 Monitorear y reportar continuamente la disponibilidad, el desempeño y la capacidad de los recursos de TI

Una gráfica RACI describe quién es Responsable, quién debe recibir cuentas (R), quién debe ser Consultado y/o Informado

Metas y métricas

Metas de actividades

- Planear y brindar capacidad y disponibilidad del sistema
- Monitoreo y reporte del desempeño del sistema
- Modelado y pronóstico del desempeño del sistema

se miden con

Indicadores clave de desempeño

- Frecuencia de los pronósticos de desempeño y capacidad
- % de activos incluidos en las revisiones de capacidad
- % de activos monitoreados a través de herramientas centralizadas

Metas de procesos

- Monitorear y medir la carga en los picos y los tiempos de respuesta de la transacción.
- Cumplir los tiempos de respuesta de los SLAs.
- Minimizar las fallas en las transacciones.
- Minimizar el tiempo sin servicio.
- Optimizar el uso de recursos de TI.

se miden con

Indicadores clave de meta de procesos

- Carga en los picos y tasas globales de utilización
- % de picos cuando se excede la utilización meta
- % de SLAs de tiempo de respuesta que no se han cumplido
- Tasa de falla de transacciones

Metas de TI

- Responder a los requerimientos del negocio de acuerdo con la estrategia del negocio.
- Asegurar que los servicios de TI estén disponibles según se requieran.
- Optimizar los recursos, la infraestructura y las capacidades de TI.

se miden con

Indicadores clave de metas de TI

- # de horas por usuario por mes, debidas a la falta de planeación de la capacidad
- # de procesos de negocio críticos no cubiertos por un plan definido de disponibilidad de servicios

TESCO

Modelo de madurez

DS3 Administrar el desempeño y la capacidad

La administración del proceso de *Administrar el desempeño y la capacidad* que *satisface el requerimiento de optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI, en respuesta a las necesidades de negocio* es:

0 No-existente cuando

La gerencia no reconoce que los procesos clave del negocio pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.

1 Inicial/Ad Hoc cuando

Los usuarios, con frecuencia, tienen que llevar a cabo soluciones alternativas para resolver las limitaciones de desempeño y capacidad. Los responsables de los procesos del negocio valoran poco la necesidad de llevar a cabo una planeación de la capacidad y del desempeño. Las acciones para administrar el desempeño y la capacidad son típicamente reactivas. El proceso de planeación de la capacidad y el desempeño es informal. El entendimiento sobre la capacidad y el desempeño de TI, actual y futuro, es limitado.

2 Repetible pero intuitivo cuando

Los responsables del negocio y la gerencia de TI están concientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.

3 Proceso definido cuando

Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.

4 Administrado y medible cuando

Hay procesos y herramientas disponibles para medir el uso del sistema, el desempeño y la capacidad, y los resultados se comparan con metas definidas. Hay información actualizada disponible, brindando estadísticas de desempeño estandarizadas y alertando sobre incidentes causados por falta de desempeño o de capacidad. Los problemas de falta de desempeño y de capacidad se enfrentan de acuerdo con procedimientos definidos y estandarizados. Se utilizan herramientas automatizadas para monitorear recursos específicos tales como espacios en disco, redes, servidores y compuertas de red. Las estadísticas de desempeño y capacidad son reportadas en términos de los procesos de negocio, de forma que los usuarios y los clientes comprendan los niveles de servicio de TI. Los usuarios se sienten por lo general satisfechos con la capacidad del servicio actual y pueden solicitar nuevos y mejores niveles de disponibilidad. Se han acordado los KGI y KPIs para medir el desempeño y la capacidad de TI, pero puede ser que se aplican de forma esporádica e inconsistente.

5 Optimizado cuando

Los planes de desempeño y capacidad están completamente sincronizados con las proyecciones de demanda del negocio. La infraestructura de TI y la demanda del negocio están sujetas a revisiones regulares para asegurar que se logre una capacidad óptima con el menor costo posible. Las herramientas para monitorear recursos críticos de TI han sido estandarizadas y usadas a través de diferentes plataformas y vinculadas a un sistema de administración de incidentes a lo largo de toda la organización. Las herramientas de monitoreo detectan y pueden corregir automáticamente problemas relacionados con la capacidad y el desempeño. Se llevan a cabo análisis de tendencias, los cuales muestran problemas de desempeño inminentes causados por incrementos en los volúmenes de negocio, lo que permite planear y evitar problemas inesperados. Las métricas para medir el desempeño y la capacidad de TI han sido bien afinadas dentro de los KGI y KPIs para todos los procesos de negocio críticos y se miden de forma regular. La gerencia ajusta la planeación del desempeño y la capacidad siguiendo los análisis de los KGI y KPIs.

TESCO

Gráfica RACI

Funciones

Actividades

Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI.
 Revisar el desempeño y la capacidad actual de los recursos de TI.
 Realizar pronósticos de desempeño y capacidad de los recursos de TI.
 Realizar análisis de brecha para identificar incompatibilidad de los recursos de TI.
 Realizar un plan de contingencia respecto a una potencial falta de disponibilidad de recursos de TI.
 Monitorear y reportar continuamente la disponibilidad, el desempeño y la capacidad de los recursos de TI.

Funciones	CEO	CFO	Gerencia de Negocio	Gerencia de TI	Gerencia de Operaciones	Gerencia de Desarrollo	Gerencia de Soporte	Gerencia de Seguridad	Gerencia de Infraestructura	Gerencia de Servicios al Cliente
Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI.			A	R	C	C	C	C		
Revisar el desempeño y la capacidad actual de los recursos de TI.			C	I	AR	C	C	C		
Realizar pronósticos de desempeño y capacidad de los recursos de TI.			C	C	AR	C	C	C		
Realizar análisis de brecha para identificar incompatibilidad de los recursos de TI.			C	I	AR		R	C	C	I
Realizar un plan de contingencia respecto a una potencial falta de disponibilidad de recursos de TI.			C	I	AR		C	C	I	C
Monitorear y reportar continuamente la disponibilidad, el desempeño y la capacidad de los recursos de TI.			I	I	AR		I	I	I	I

Una gráfica RACI denota a quién es Responsable, quién debe recibir cuentas (R), quién debe ser Consultado y/o Informado.

Metas y métricas

Metas de actividades

- Planear y brindar capacidad y disponibilidad del sistema.
- Monitoreo y reporte del desempeño del sistema.
- Modelado y pronóstico del desempeño del sistema.

se miden con

Indicadores clave de desempeño

- Frecuencia de los pronósticos de desempeño y capacidad.
- % de activos incluidos en las revisiones de capacidad.
- % de activos monitoreados a través de herramientas centralizadas.

Dirigen

Metas de procesos

- Monitorear y medir la carga en los picos y los tiempos de respuesta de la transacción.
- Cumplir los tiempos de respuesta de los SLAs.
- Minimizar las fallas en las transacciones.
- Minimizar el tiempo sin servicio.
- Optimizar el uso de recursos de TI.

se miden con

Indicadores clave de meta de procesos

- Carga en los picos y tasas globales de utilización.
- % de picos cuando se excede la utilización meta.
- % de SLAs de tiempo de respuesta que no se han cumplido.
- Tasa de falla de transacciones.

Dirigen

Metas de TI

- Responder a los requerimientos del negocio de acuerdo con la estrategia del negocio.
- Asegurar que los servicios de TI estén disponibles según se requieran.
- Optimizar los recursos, la infraestructura y las capacidades de TI.

se miden con

Indicadores clave de metas de TI

- # de horas por usuario por mes, debidas a la falta de planeación de la capacidad.
- # de procesos de negocio críticos no cubiertos por un plan definido de disponibilidad de servicios.

TESCO



Entregar y dar soporte

Garantizar la continuidad del servicio

Modelo de madurez

DS4 Garantizar la continuidad del servicio

La administración del proceso de Garantizar la continuidad del servicio que satisfaga el requerimiento de TI del negocio para asegurar el mínimo impacto al negocio en caso de interrupción de un servicio de TI es:

0 No-existente cuando

No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.

1 Inicial/Ad Hoc cuando

Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternativas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.

2 Repetible pero intuitivo cuando

Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.

3 Proceso definido cuando

La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir capacitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.

4 Administrado y medible cuando

Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda capacitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.

5 Optimizado cuando

Los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de disponibilidad y la continua planeación de la continuidad están totalmente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirá como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática. La gerencia ajusta la planeación de continuidad como respuesta a los KGIs y KPIs.



TESCo

DS7 Educar y entrenar a los usuarios

Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya:

- Estrategias y requerimientos actuales y futuros del negocio.
- Valores corporativos (valores éticos, cultura de control y seguridad, etc.)
- Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)
- Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias.
- Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.

Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

Al finalizar la intervención, evaluar el contenido de la intervención respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

GRAFICA RACI

[illegible]

Una política RACI identifica quién es Responsable, quién debe ser consultado (C), quién debe ser Consultado y/o Informado.

Metas de actividades

- Establecer plan de entrenamiento
- Organizar el entrenamiento
- Impartir el entrenamiento
- Monitorear y reportar la efectividad del entrenamiento

se miden con

- Frecuencia de actualizaciones del programa de capacitación.
- Lapso de tiempo entre la identificación de la necesidad de capacitación y la impartición de la misma.

Dirigen

- Establecer un programa de capacitación para usuarios a todos los niveles utilizando los métodos con mayor rentabilidad.
- Transferir el conocimiento a los usuarios de las aplicaciones y soluciones tecnológicas.
- Incrementar la conciencia sobre los riesgos y las responsabilidades involucrados en el uso de soluciones y aplicaciones tecnológicas.

se miden con

- # de llamadas de soporte para capacitación o para responder preguntas
- % de satisfacción de los interesados a quienes se les brindó capacitación
- % de empleados capacitados.

10/10/2019

- Garantizar la satisfacción de los usuarios finales con ofrecimiento de servicios y niveles de servicio.
- Garantizar el uso apropiado y el desempeño de las aplicaciones y soluciones tecnológicas.
- Optimizar la infraestructura, los recursos y las capacidades de TI.

se miden con

- Mejoras medidas en la productividad de los empleados como resultado de un mejor entendimiento de los sistemas.
- Aumento de la satisfacción del usuario con la introducción de servicios, sistemas o nuevas tecnologías.