ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DE CONCURSO DE MÉRITOS Y OPOSICIÓN EN LA GOBERNACIÓN DE LA PROVINCIA DEL GUAYAS BASADO EN EL ESTÁNDAR ISO: 27001"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Autores:

ING. MARIUXI JACQUELINE CÓRDOVA ALDÁS

ING. BRENNERO DANIEL PARDO CENTANARO

GUAYAQUIL – ECUADOR

Año: 2017

AGRADECIMIENTO

El presente trabajo, aparte de ser un escrito de investigación, es un libro donde queda impregnada la emoción de su autor y donde probablemente muchas personas van a pasar por ella.

Doy gracias a Dios por poner a sus ángeles en este camino de titulación; por ser Él el personaje principal de muchas metas en mi vida. Agradezco por haber puesto al Abg. Julio César Quiñonez, quien dio carta abierta a la realización de mi tesis en la Gobernación; al Ing. Lenin Freire quien con cariño, por segunda vez, es autor principal de otro trabajo de tesis, así como brindarme sus conocimientos para hacer un mejor trabajo de titulación; a mis maestros de la maestría quienes abrieron mis conocimientos con cada una de sus

clases; a mi abuela Mina que sin estar presente físicamente dejó en mi corazón clavado el motor de la auto superación a través del esfuerzo.

Agradezco sobre todo a mis padres Pepe y Violeta que siempre han sido mi motor al querer darles lo mejor de mí, sin permitirme fallarles para que se sientan orgullosos de la persona que han formado. A mis amigos y compañeros que no sólo dieron ideas para mejorar el presente trabajo, sino que fueron ese equilibrio para tener una estabilidad tanto profesional como emocional.

Ing. Mariuxi Córdova Aldás

AGRADECIMIENTO

Agradezco a mi familia, motor principal de mi ser, quienes con sus consejos me han enseñado valores como la honestidad y la perseverancia. El saber que uno nunca deja de aprender y adquirir conocimientos nuevos terminados una etapa de la vida. A mi abuelo, que, aunque no esté físicamente conmigo, sé que me está viendo desde el cielo orgullo del nieto que ha formado. Agradezco a mis profesores de maestría que con sus enseñanzas me han llenado de nuevos conocimientos e ideas para el ámbito tanto académico como profesional. A mis amigos, quienes sus anécdotas y enseñanzas también, me hicieron reforzar mis

conocimientos y adentrarme en nuevas formas de ver las cosas.

Agradezco al Ing. Lenin Freire, lo cual es grato, al volver a contar con su conocimiento para avanzar en este trabajo de titulación.

Agradezco a Dios, quien me llena de fuerzas para continuar siempre mejorándome como profesional y sobre todo como ser humano.

Ing. Brennero Pardo Centanaro

DEDICATORIA

La vida se encuentra llena de retos, los cuales uno de ellos es la culminación de nuestra maestría para obtener ese título tan anhelado. Al ir avanzando con el presente trabajo nos hemos dado cuenta que, más allá de ser un reto a nivel académico, es la base no sólo para nuestro entendimiento en el campo que decidimos especializarnos que es la seguridad informática, sino para lo que concierne a la vida y nuestro futuro.

Dedicamos esta tesis a todos aquellos que han sido nuestra mano derecha y apoyo incondicional durante todo este tiempo de elaboración de la misma; por su desinteresada ayuda a nuestro proyecto de titulación. Son y fueron

nuestro pilar fundamental en nuestra formación como magisters.

Ing. Mariuxi Córdova

Ing. Brennero Pardo

TRIBUNAL DE SUSTENTACIÓN

_____

DIRECTOR MSIG/MSIA

MSG. LENIN FREIRE

_____

DIRECTOR DE PROYECTO DE GRADUACIÓN

MSG. LENIN FREIRE

_____

MIEMBRO DEL TRIBUNAL

MSG. ROBERT ANDRADE

DECLARACIÓN EXPRESA

“Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual".

_____

Ing. Mariuxi Córdova Aldás

DECLARACIÓN EXPRESA

“Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual".

_____

Ing. Brennero Pardo Centanaro

RESUMEN

El presente trabajo de Titulación de la Maestría de Seguridad Informática Aplicada de la Facultad de Ingeniería en Electricidad y Computación, nace del convenio con la Gobernación de la Provincia del Guayas, cuya finalidad es la de implementar un esquema de seguridad de la información para el proceso de concurso de méritos y oposición en la Gobernación de la Provincia del Guayas basado en el estándar ISO 27001.

Al realizar el análisis de riesgo y vulnerabilidad a las áreas de Recursos humanos y Tecnología de la información y la comunicación de la Gobernación de la provincia del Guayas, se preparó al personal para actuar antes las amenazas informáticas que está expuesto el sector público en especial en el proceso de Concurso de méritos y oposición.

Finalmente, este aporte profesional que se realiza a la Gobernación de la provincia del Guayas, está enfocada a mejorar la seguridad de la información utilizando las herramientas tecnológicas adecuadas para la ejecución del proceso.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

BPMN: Business Process Model and Notation).

CIS: Center for Internet Security.

DISA: Defense Information Systems Agency.

INM: Instituto Nacional de la Meritocracia.

LOSEP: Ley Orgánica del Servicio Público.

MBSA: Microsoft Baseline Security Analyzer

MDT: Ministerio del Trabajo.

PEO: Procedimientos estándar de operación.

PHVA: Ciclo Planificar-Hacer-Verificar-Actuar.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SIITH: Sistema Integrado de Información del Talento Humano.

STIG: Security Technical Implementation Guide.

UATH: Unidad de Administración del Talento Humano.

UTIC: Unidad de tecnología de la información y la comunicación.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La Gobernación de la Provincia del Guayas es una institución pública que direcciona y orienta las políticas del Gobierno Nacional en la provincia del Guayas. Actualmente, la institución no mantiene un sistema de gestión de calidad. En el año 2015, la Gobernación del Guayas se encontró con la necesidad de crear 83 partidas de nombramiento permanente cumpliendo con el Art. 1 y Art. 2 del Acuerdo Interministerial N° MDT-2015-002 donde se indica que el 20% debe estar bajo la modalidad de contrato de servicio ocasional y el 80% con la modalidad de nombramiento permanente.

Los concursos de méritos y oposición fueron creados para que toda la ciudadanía ecuatoriana, que cumpla el perfil del puesto ofertado, pueda participar y para que, la unidad de talento humano de cada una de las diferentes instituciones públicas realice un proceso transparente de selección de personal, el cual culminará en la obtención de un puesto de nombramiento permanente mediante selección, pruebas, entrevistas finalizando con la declaratoria del ganador del concurso.

La Gobernación de la Provincia del Guayas empieza la planificación para selección de personal por medio del proceso de méritos y oposición el 1 de marzo de 2016, el cual tiene una duración de un año y medio para tener a los 83 ganadores de las partidas a lanzarse. Para lograr este objetivo se realizó un análisis de los puestos y los procesos con sus respectivas etapas. Teniendo como herramienta las normativas creadas por el instituto de la Meritocracia y Ministerio de Relaciones Laborales.

En vista que la Gobernación de la Provincia del Guayas tiene que lanzar a concurso las 83 partidas con un proceso de mérito y oposición de manera transparente, se propone el desarrollo de un proyecto que asegure que todo el proceso en especial el uso de herramientas de tecnologías para el almacenamiento de la información sea utilizada de manera segura, además el control de los accesos. El proceso abarcará las áreas operativas, de sistemas y selección, de manera especial los subprocesos claves: Planificación del concurso, ejecución de pasos previos, convocatoria, mérito y oposición, banco elegible que son los que permiten a la Gobernación de la Provincia del Guayas hacer la selección del personal con nombramiento permanente.

Para el desarrollo de la planificación de la seguridad informática aplicada, se contará con el apoyo de la Psicóloga Dennys Días Fuentes - jefa de la unidad de Recursos Humanos y todo el personal operativo del departamento con un tiempo de entrega de 6 meses a partir de la aprobación del acta de autorización del proyecto.

La Gobernación de la provincia del Guayas tiene como necesidad mantener en condiciones de control la información que se maneja en los concursos de méritos y oposición que se ejecutan a través de las herramientas del sistema, con la finalidad que quede de forma transparente un ganador por cada partida lanzada. Teniendo todo esto definido se establece como objetivo desarrollar un proyecto “Implementación de un esquema seguridad de la información del proceso de concursos de méritos y oposición, en la Gobernación de la provincia del Guayas basados en el estándar ISO 27001” con fundamento en el desarrollo de los procesos de la Unidad de Recursos Humanos.

Se estableció en forma consecuente la planificación y definición del alcance del proyecto, las diferentes actividades que permiten generar los entregables finales y se identificó los roles y responsabilidades del equipo del proyecto, al igual que los medios y mecanismos bajo los cuales se estructuran y coordinará una comunicación efectiva de todos los eventos durante la ejecución del proyecto en sus diferentes fases; para que finalmente se logre contar con el sistema de gestión para la seguridad de la información.

La metodología para realizar el levantamiento de información para la planificación del proyecto se basó en entrevistas, hechos pasados y procesamiento de datos; lo cual se sustenta en el criterio de los responsables de los procesos a nivel interno de la Gobernación de la Provincia del Guayas especialmente en las áreas de Recursos humanos y tecnología de la información, así como de las diferentes herramientas que son utilizadas para este proceso y todo lo disponible en Gobernación de la provincia del Guayas, como informes de procesos pasados.

Como parte de las expectativas, se espera que el equipo de trabajo del proyecto esté conformado por técnicos y profesionales de los diferentes departamentos de la Gobernación de la provincia del Guayas.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La Gobernación de la provincia del Guayas pasa por un proceso de selección de méritos y oposición del periodo 2016 al 2017, y no cuenta con sistema de seguridad informática para demostrar a gran escala la transparencia del proceso. Durante la selección del Ganador del concurso se generan actas, reportes, datos y material de diferente índole que suma la importancia al proceso. Al mejorar este proceso brindamos a los usuarios confiabilidad de los Resultados, y transparencia de la institución con la información.

El acceso no autorizado a la información se ha vuelto más fácil, debido a los métodos existentes para extraer información. Esto hace más complejo salvaguardar la información y sus métodos de transmisión. Debido a que es un proceso público tiene el riesgo de que la información sea interceptada, robada o modificada por personas sin la autorización, lo cual afecta a la transparencia del proceso.

Por lo anteriormente mencionado es necesaria la implementación de proceso, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar que accedan a la información las personas que estén designadas para su uso. Y por este motivo la gobernación del Guayas opta por aceptar la propuesta de titulación para la implementación de los controles de seguridad informática utilizando la norma ISO 27001 en el proceso de concursos de méritos y oposición, creando políticas de seguridad y proceso que se sugiere a la organización.

1.2. Descripción del problema

Actualmente la Gobernación de la provincia del Guayas no cuentan con las medidas, los controles, procedimientos de seguridad necesarios para resguardar a sus activos de información (Software, personas, documentos, dispositivos físicos, Figuraes y servicios) que están

expuestos a altos niveles de riesgo frente a las amenazas que existen tales como:

- Desastres del entorno.
- Amenazas de software.
- Amenazas de hardware.
- Amenazas en la red.

Corriendo el riesgo de sufrir accesos no autorizados por no tener los controles respectivos poniendo en la cuerda floja los principios de la seguridad de la información que son: confidencialidad, disponibilidad e integridad. Esto se pudo constatar con la primera inspección realizada a la Gobernación de la provincia del Guayas.

Entre los problemas que se encontraron en la inspección son:

- El acceso no autorizado a los datos de concurso de mérito y oposición.
- Interceptación de correos electrónicos.
- Usos comerciales no éticos.
- Ausencia de estructura de políticas, normas y procedimientos internos.
- Plan de continuidad.
- Usuarios con poca capacitación.
- Navegación insegura.
- Mal uso de dispositivo de almacenamiento portátil.

- Falta de cifrado adecuado.
- Uso de conexión Wireless.
- Contraseñas inseguras.
- Falta cerradura en los archiveros donde se almacena las carpetas del procedimiento.

Al considerar y mitigar estos riesgos en la Gobernación podemos salvaguardar los activos de la información.

1.3. Solución propuesta

La información que maneja la Gobernación del Guayas con respecto al proceso de méritos y oposición es de gran importancia para la transparencia del ganador del concurso. Para lo cual se implementa un esquema de seguridad de la información para este proceso, y de esta manera preservar las siguientes propiedades de la información.

Confidencialidad: Evitar que la información sea manipulada por personas, entidades o procesos no autorizados. Integridad: Proteger la precisión y complejidad de los datos.

Disponibilidad: Asegurar que la información este accesible y autorizable bajo petición de los usuarios autorizados.

La adopción de este esquema de seguridad de la información es una decisión estratégica para la unidad de Recursos Humanos y Tecnología de la información, con el fin de brindar la transparencia que este proceso debe tener. A la vez hacer un plan de riesgo de seguridad basada en la norma ISO 27001:2013.

1.4. Objetivo general

Reducir y mitigar los riesgos de los activos de la información del proceso de Méritos y Oposición de la Gobernación de la Provincia del Guayas. Que ponen el peligro la transparencia del ganador del concurso.

1.5. Objetivos específicos

- Implementar una política de seguridad para cada uno de los subprocesos.
- Monitorear y gestionar los incidentes y vulnerabilidades de la seguridad de la información para reducir en un 90%.
- Ejecutar controles de seguridad para reducir los riesgos en un 90%.
- Elaborar el sistema de gestión de seguridad de la información basada en la norma ISO 27001.

- Gestionar y controlar el 100% de los documentos de seguridad de la información según la norma ISO 27001.

1.6. Alcance

El alcance del presente trabajo de titulación, abarca un diseño de un sistema de gestión de seguridad de la información, basada en la norma ISO 27001 y está dirigido al proceso de concursos de méritos y oposición en la Gobernación de la provincia del Guayas, El proyecto cubrirá los aspectos a tener en cuenta en los estándares, procedimientos, normas y medidas que empleen tecnología que permita asegurar la transparencia de la elección del Ganador de concurso.

El alcance del proyecto es solo del proceso detallado anteriormente. Fundamento principal para demostrar la veracidad y credibilidad de la transparencia de la elección del funcionario a obtener su nombramiento permanente. Este proceso de Concursos de méritos y oposición abarca siete subprocesos que son:

- Convocatoria,
- Mérito,
- Oposición,
- Pruebas de conocimiento técnicos,
- Pruebas psicométricas,

- Entrevista, y
- Declaratoria de ganador de concurso.

1.7. Metodología

Para el análisis y gestión de riesgos del proceso de méritos y oposiciones de la Gobernación de la provincia del Guayas, se va utilizar la metodología MAGERIT. Esta metodología utiliza un conjunto con varias herramientas que permiten llevar a cabo el análisis con mayor automatización (PILAR).

Características de la metodología Margerit:

- Concienciar a los involucrados del proceso de méritos y oposición de la Gobernación de la provincia del Guayas de la existencia de Riesgos y de la necesidad de Gestionarlos.
- Ofrecer un método sistemático para realizar los riesgos de uso de la tecnología de la información y comunicación.
- Descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control indirecto.
- Preparar a la Gobernación del Guayas para algún proceso de auditorías futuras.

El análisis de riesgo usando la metodología margerit revisa como están protegidos los activos y por lo tanto ayuda a la determinación de un plan de seguridad que satisfaga los objetivos propuestos en el proyecto.

MAGERIT se divide en 10 fases que se detallará a continuación:

- **Fase 1 Toma de datos:** No se analiza riesgos, pero se determina los elementos sobre los que se aplicará la metodología, se realiza un estudio sobre los procesos de la organización sobre todo en los procesos críticos y los riesgos que intervienen en ellos.

- **Fase 2 Dimensionamiento:** Esta fase es Importantee para la organización, porque una falla en el establecimiento de los parámetros y no se ajustará en la situación actual.

- **Fase 3 Análisis de Activos:** Identificar los activos de la organización como: Activos físicos, Activos Lógicos, Activos de personal, Activos de infraestructura, Activos intangibles.

- **Fase 4 Análisis de Amenaza:** Se estudia la amenaza de la funcionabilidad de los activos. Existen 4 clasificaciones de amenazas: Accidentes, Errores, Amenazas intencionales presenciales y amenazas intencionales remotas.

- **Fase 5 Establecimiento de vulnerabilidades:** Establecer las frecuencias en la que ocurre las amenazas sobre los activos.

- **Fase 6 valoración de impacto:** Establecer los daños que se produce en la Gobernación del Guayas como: Incidencia de una amenaza sobre un activo y efecto sobre los activos.

- **Fase 7 análisis de riesgo:** Con las fases anteriores se puede detectar el análisis del riesgo, utilizando la formula Riesgo=Valor del activo X Vulnerabilidad X Impacto.

- **Fase 8 influencia de Salvaguardia:** Eligen soluciones de seguridad para los riesgos encontrados en las fases anteriores. Existen 2 tipos de Salvaguardia Preventiva y Correctivas.

- **Fase 9 Análisis de riesgo Efectivo:** Resultados de aplicar las salvaguardias.

- **Fase 10 Gestión de riesgo:** Escoger las vías de acción para cada Riesgo. Estrategias de Gestión de Riesgo son: Reducirlo, Transferirlos, Aceptarlos.

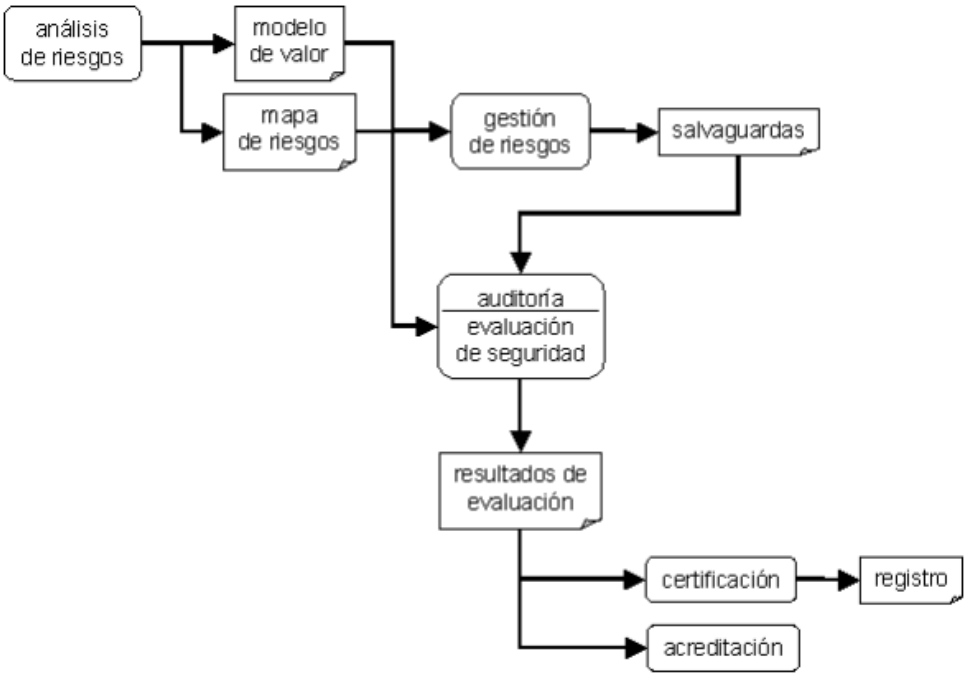


FIGURA 1.1: Fases de Margerit. Fuente: Metodología de análisis y gestión de riesgos de los sistemas de información (Madrid, octubre 2012)

CAPÍTULO 2

MARCO TEÓRICO

2.1. Seguridad Informática

La seguridad en la informática es un tema actual muy controversial debido a que se escuchan en los medios acontecimientos como robo de información, robo de base de datos, manipulación en la información, etc. Y es que, si no se tiene resguardada la información o si es puesta en manos no autorizadas, la institución o empresa puede correr grandes riesgos económicos y/o de Figura negativa frente a la sociedad. No existen sistemas cien por ciento seguros.

Definiciones para el término seguridad hay muchas. Entre ellas tenemos una de **Villalón Huerta** quien define a la seguridad como una "característica que indica que un sistema está libre de todo peligro, daño o riesgo" (Villalón Huerta, 2002). Cuando se habla del término seguridad, la palabra fiabilidad va de la mano. Esto es, la probabilidad de que un sistema o programa se comporte tal y como el usuario espera que se comporte. La fiabilidad se basa en tres pilares los cuales son:

- **Confidencialidad:** cuya información es accesada por personal autorizado y de una manera verificada.

- **Integridad:** donde la información debe sólo ser modificada por personal autorizado.

- **Disponibilidad:** la información debe estar disponible a las personas que la necesiten o requieren en ese momento.

Una característica adicional que con lleva el término seguridad es:

- **No repudio:** cuando la persona no puede negar lo que ha hecho o dicho.

- El objetivo de la seguridad es proteger los elementos de información (también llamados activos o recursos) que forman parte de un sistema. Estos elementos se dividen en tres grupos:

- **Datos e información:** información valiosa (Finanzas, RRHH, correos electrónicos, llamadas telefónicas, informes, reportes, base de datos, mensajería instantánea) almacenada en el hardware haciendo uso del software del negocio o institución.

- **Sistemas e infraestructura:** es aquí donde se almacenan y viajan los datos e información. Son equipos físicos tales como equipos de red (switches, firewalls, routers, IPS), computadoras, laptops, servidores, celulares, usb, micro sd,… Así como los programas o herramientas destinadas al uso del personal.

- **Personal:** personal que tiene acceso a los datos e información tales como personal técnico, junta directiva, administración, coordinación, ventas, importación, inventario, logística.

Es por esto que los datos son el activo informático más indispensable en cualquier organización debido a que la infraestructura, aunque es cara, se la puede reponer; el sistema, puede ser tanto costoso como no, pero

se lo puede adquirir, mientras que los datos al ser modificados, robados o destruidos pueden ocasionar daños y pérdidas incalculables y la dificultad para reponerlos puede ser grande.

Existen términos que van de la mano con un activo como vulnerabilidad, amenaza, impacto, riesgo, control.

La vulnerabilidad es una debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004] es una debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Una amenaza según [ISO/IEC 13335-1:2004]: es una causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o la organización.

Según Wikipedia, la probabilidad es "una medida de la certidumbre asociada a un suceso o evento futuro y suele expresarse como un número entre 0 y 1 (o entre 0% y 100%)" que mide la frecuencia con la que se obtiene un Resultados (o conjunto de Resultados) al llevar a cabo un experimento aleatorio, del que se conocen todos los Resultados posibles, bajo condiciones suficientemente estables. Un suceso puede

ser improbable (con probabilidad cercana a cero), probable (probabilidad intermedia) o seguro (probabilidad 1).

Cuando un sistema presenta una vulnerabilidad y está presente una amenaza, aparece un riesgo asociado, es decir, la probabilidad de que el evento llegue a materializarse.

El impacto es la medida o grado del daño sobre un activo producto de la materialización de una amenaza. Esta afecta cualitativa o cuantitativamente las actividades/procesos del negocio principalmente en los siguientes principios: intercepción (invade la confidencialidad), modificación (invade la integridad) o interrupción (invade la disponibilidad) pueden generarse por personas tales como usuarios, exempleados, hackers, por código malicioso como los troyanos, virus, gusanos, ramsomware, spam, spyware, y por el medio (incendios, terremotos, inundaciones, cortes de energía).

Tabla 1: Tabla de impacto

Detalle del Impacto	C	I	D
Impacto 1	-	3	1
Impacto 2	2	3	5
Impacto 3	4	5	3

Datos obtenidos en el campo (Elaboración propia)

Tabla 2: Tabla de impacto de activos

	Amenaza	Vulnerabilidades	Prob	Impacto	Detalle Impacto
Servidor de dominio de red	Ingreso a personal no autorizado.	Control de acceso físico pobre.	Alta.	Bajo.	Impacto 1
	Cese de operación del equipo.	Servicios adicionales instalados. Actualizaciones instaladas sin previo testing. Documentación incompleta. Renovación del hardware. Falta de mantenimiento.	Media. Muy Alta. Alta. Muy Baja. Baja.	Alto	Impacto 2
	Rendimiento	Ambiente no	Media.	Medio.	Impacto 3.

	bajo del servidor.	adecuado para operación. Falta de mantenimiento. Servicios adicionales instalados.	 Alta. Muy Alt.		

Datos obtenidos en el campo (Elaboración propia)

Tabla 3*:* Tabla Análisis CID (Confiabilidad, integridad, Disponibilidad)

Activo	Vulnerabilidades	Probabilidad	Amenaza	Impacto	C	I	D
	Servicios adicionales instalado	Muy Baja (01)	A1	Bajo (B)			
	Actualizaciones instaladas sin previo testing/prueba	Muy Alta (10)		Muy Alto (MA)	-	2	5

Servidor de dominio de red	s						
	Documentación incompleta	Alta (08)		Muy Bajo (MB)			
	Renovación del hardware	Media (05)		Alta (A)			
	Falta de mantenimiento	Alta (08)		Muy Alta (MA)			
	Ambiente no adecuado para operación	Baja (03)		Medio (M)			

Datos obtenidos en el campo (Elaboración propia)

A las medidas que eliminen la vulnerabilidad o la amenaza, o disminuya el riesgo o impacto asociados, se les denomina defensa o controles.

Para protegernos de estas amenazas nuestra primera línea de defensa son las políticas de seguridad, que son documentos que definen las acciones a tomar y directrices organizativas con respecto a la seguridad. Estas políticas, a su vez, son establecidas en mecanismos de seguridad.

Los mecanismos de seguridad cuentan con tres fases:

- **Prevención:** se evitan las desviaciones referentes a la política de seguridad previamente establecida.

- **Detección:** donde se detectan si son producidas dichas deviaciones y,

- **Recuperación:** tras haber ocurrido una desviación recuperar el funcionamiento correcto.

Los activos existen en un entorno y esto, de por sí, los expone a amenazas tales como:

- Casos de naturaleza (incendios, terremotos, inundaciones, tormentas, etc.)
- Intencionados por el hombre (incendios, demoliciones, robos, etc.).

2.1.1. Ataques informáticos

Las maneras de atacar una red o un sistema de la red pueden ser tanto de forma activa (ataques basados en escuchar los datos que son transmitidos, pero sin modificarlos) y pasiva (ataques que

modifican y/o alteran la información ya interceptada para realizar daños).

Se muestra a continuación una lista de ataques informáticos originados por personas internas y externas:

- Análisis de tráfico.
- Ataque de suplantación de identidad.
- Detección de vulnerabilidades.
- Introducción de código malicioso.
- Detección de vulnerabilidades en los sistemas de red.
- Robo de información.
- Denegación de servicios.
- Conexiones no autorizadas.
- Modificación del contenido y secuencia de los mensajes transmitidos.
- Denegación de servicios distribuido.

2.1.2. Ataques comunes a una red LAN

Algunas de las vulnerabilidades más comunes y posibles puntos que sirven como puerta de ingreso para los intrusos y poder así acceder a los recursos de las redes gubernamentales están:

- **Contraseñas por defecto o ninguna:** esto hace que el intruso sepa las contraseñas predeterminadas por el fabricante. Este tipo de “prácticas” son más comunes en hardware tales como switches, routers y firewalls, así como en las conFiguraciones los servidores cuya contraseña de usuario predeterminado root (el cual es el administrador) ponen contraseñas como 12345 por defecto.

- **Vulnerabilidad de servicios:** el atacante busca una debilidad en un servicio de la red. Siendo esta vulnerabilidad conocida por el agresor, pone en riesgo el/los sistemas(s) y los datos que pueda contener y otros sistemas dependientes. Entre estos servicios están los basados en http tales como CGI los cuales son vulnerables a comandos ejecutados de manera remota y al acceso de Shell interactivo. Asimismo, a través de http se puede acceder a archivos de conFiguración y mapas de redes que pueden ser leídos por el atacante para iniciar o negar el ataque del servicio convirtiendo las peticiones de usuarios validos como no disponibles a ser atendidas. Los administradores de los servidores no deben operar como usuarios root y estar atentos a los parches y actualizaciones de

los sistemas operativos que usa, así como de las aplicaciones de los proveedores.

- **Vulnerabilidades de aplicaciones:** puede existir fallas en las aplicaciones de trabajo (herramientas de edición, correo electrónico). Cuenta como vulnerabilidades el tener el usuario de la estación de trabajo privilegios administrativos sobre el sistema operativo. Las máquinas de los usuarios son más expuestas debido a que ellos no tienen experiencia alguna para detectar o evitar si la información está siendo comprometida. Es de suma importancia informar a los usuarios de los riesgos que se correo al instalar software no autorizado o al abrir adjuntos de correo no deseado.

- **Intercepción pasiva:** Recolección de datos entre dos nodos activos en la red. Este tipo de ataques funciona con protocolos de transmisión de texto plano como telnet, ftp y http. Para poder llevar a cabo este tipo de ataque, el atacante debe tener acceso al sistema dentro de la LAN, anterior a un ataque activo tales como la suplantación de IP o tercero interpuesto conocido también como man-in-the-middle.

- **Ataque distribuido de denegación de servicios (DoS):** el atacante tiene a su cargo maquinas Botnets las cuales envían paquetes no autorizados al host de destino, haciendo que los recursos no estén disponibles para usuarios llegítimos. Existen herramientas que ayudan a los administradores a detectar y evitar este tipo de ataques como snort.

2.2. Estándares y normas aplicables a la seguridad informática

2.2.1. Ciclo de Deming (Ciclo PHVA)

Una de las herramientas de mejoras continuas es el ciclo de control PVHA, el cual inicialmente fue aplicado para el desarrollo de nuevos productos. En la actualidad se aplica a cualquier operación para garantizar la mejora continua. Este ciclo lleva el nombre de Deming debido a que fue este quien lo presentó a directores de empresas japonesas. De manera general trata de una secuencia lógica que corresponde de 4 pasos que se detallan a continuación:

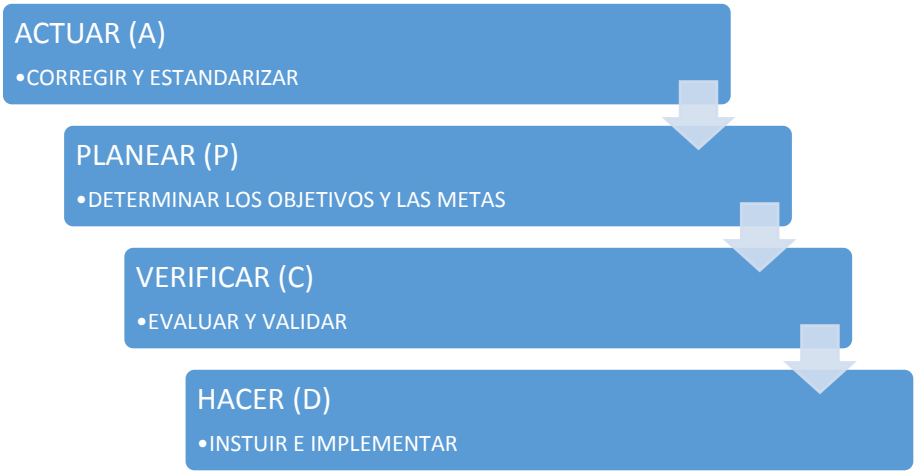


FIGURA 2.2: Ciclo de Deming. Fuente: Los autores

Hacer:

Involucra comunicar los Resultados de la planeación (objetivos, estrategias, políticas, programas y métodos de trabajo) a todos los implicados y la ejecución de las actividades y el registro de los datos.

Actuar:

Involucra tomar decisiones relacionadas con el estado de actividades determinado en la verificación.

Planear:

Lo primero que se definen son las políticas, las cuales deben estar acorde a las necesidades y expectativas de las partes

interesadas. Estas son el marco para establecer los objetivos y las metas, los cuales llevan al desarrollo de estrategias, programas y métodos de trabajo.

Verificar:

De manera periódica se comparan los avances, las tendencias y los Resultados obtenidos con relación a lo proyectado.

El ciclo de control fue enriquecido luego por el Dr. Kaoru Ishikawa, quien lo definió como un proceso formado por seis pasos.

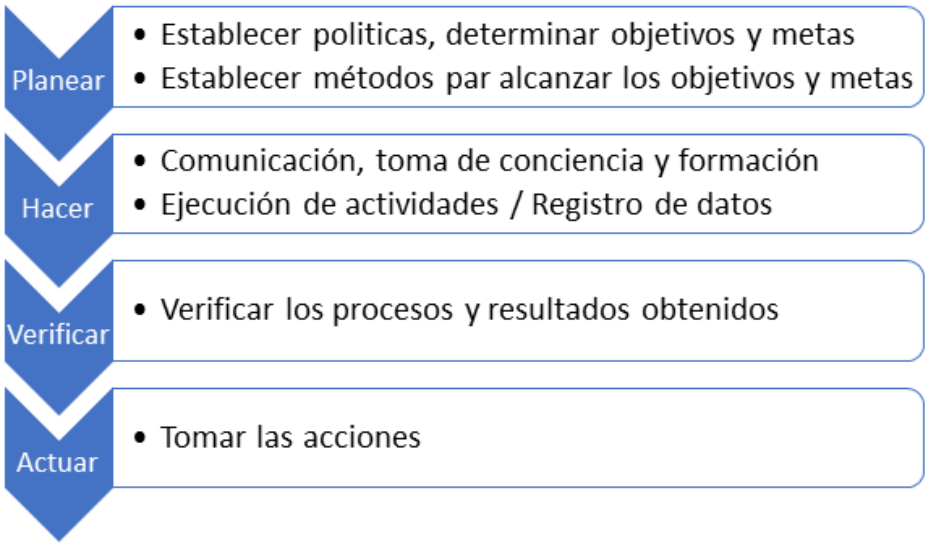


FIGURA 2.3: 6 Pasos del ciclo de control. Fuente: Los autores

Planear: establecer políticas, determinar objetivos y metas

La alta dirección es la encargada de **establecer las políticas** las cuales representan el marco referencial para establecer o **determinar los objetivos** y **metas**. Estas políticas deben establecerse de manera correcta, debido a que si no se lo hace las metas y objetivos no se pueden definir de manera coherente.

Las políticas son directrices que guían los esfuerzos de las personas que forman parte de la acción en un periodo dado. Deben ser priorizadas sin representar una carga pesada que haga difícil su puesta en marcha.

Los objetivos constituyen los propósitos y metas. Se deben expresar con uno o varios indicadores los cuales tienen que ser concretos, explícitos y claros para que sean entendidos por los implicados. Se usan las siguientes acciones: evaluar, aumentar, incrementar, mantener, reducir o disminuir; eliminar, certificar, implementar, etc. seguida con el objeto de la acción.

En las metas se asignan los plazos, responsables y rangos numéricos, si el caso lo amerite. Se debe garantizar la colaboración de todas las áreas convenientes.

Los aspectos relevantes que se pueden identificar entre las políticas, objetivos y metas son:

- Armonizan entre sí.
- Redacción concisa y clara.
- Documentación y distribución entre las partes implicadas.
- Toma de conciencia de responsabilidad para cumplimiento en las personas involucradas.
- Señalan un camino concreto de acción a seguir.

Planear: Establecer métodos para alcanzar los objetivos y metas.

No se puede alcanzar objetivos y sus metas si no se implantan métodos, planes y programas para conseguirlos. Esto se apoya en la cita del Dr. Ishikawa: “Si se fijan metas y objetivos, pero no se acompañan con métodos para alcanzarlos, el control de la calidad acabará por ser un simple ejercicio mental”.

Para definir y documentar la estrategia de los programas, métodos o planes de trabajo se deben hacer algunas precisiones:

- Satisfacer los objetivos y las metas establecidas, es decir, la satisfacción de las necesidades de clientes (internos y externos) y el resto de las partes interesadas.
- Considerar la eficiencia, eficacia y factor humano.
- Definir indicadores de control y de verificación.
- Considerar métodos de seguimiento y medición.
- Revisar periódicamente ya que el análisis de los procesos y la revisión de las normas son la base del progreso tecnológico de la institución/empresa.

Indicadores de verificación y control

Los indicadores de verificación son índices numéricos establecidos sobre los factores causales que afectan al Resultados. Necesitan ser administrados para garantizar la calidad de los productos/servicios.

Los indicadores de control son índices numéricos definidos sobre los Resultados del proceso. Estos están asociados a las seis dimensiones de la calidad: entrega, calidad intrínseca, motivación, precio, seguridad, medio ambiente y precio.

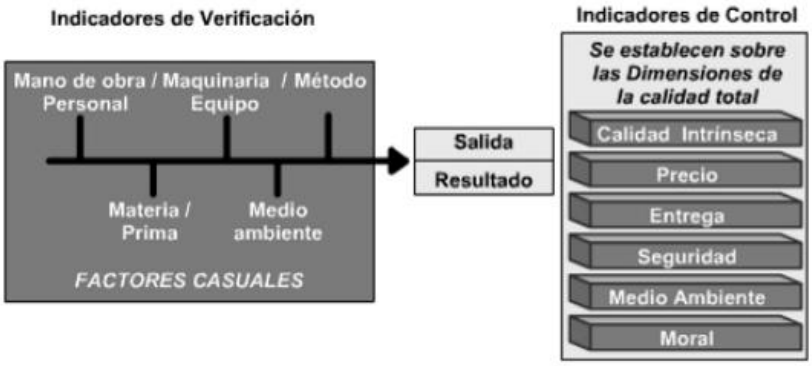


FIGURA 2.4: Indicadores de verificación y control.

Tomado de Universidad TecVirtual del Sistemas Tecnológico de Monterrey (Mexico, 2012)

En este punto termina la etapa de planeación (planear) y comienza la ejecución (hacer) de las actividades planificadas, como parte del ciclo PHVA.

Comunicación, toma de conciencia y formación

Las personas con facultades de autoridad y dirección deben cumplir con la responsabilidad de mantener informado al personal, garantizando comprenda su rol y responsabilidades y desarrolle las aptitudes necesarias para cumplir con las actividades que se le encomienden.

Esta comunicación no se refiere a cursos de capacitación, reuniones formales o decir las reglas básicas. Implica el desarrollo de competencias en el trabajo práctico para así poder delegar la responsabilidad y autoridad como construir el facultamiento (empowerment).

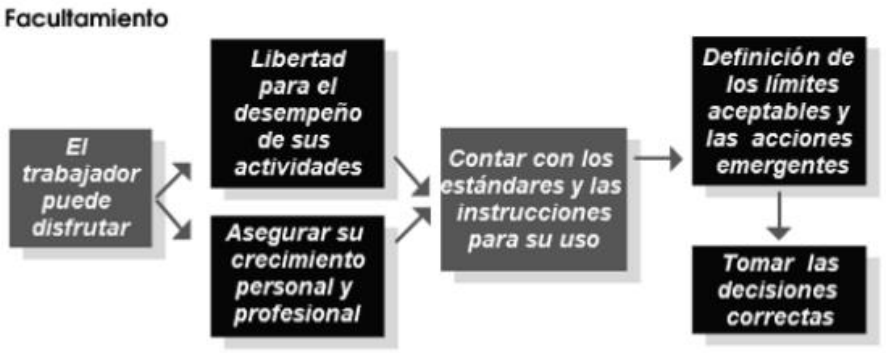


FIGURA 2.5: Facultamiento. Tomado de Universidad Tecvirtual del Sistemas Tecnológico de Monterrey (Mexico, 2012)

Ejecución de las actividades / Registro de datos

Las actividades se deben ejecutar de acuerdo con los programas, procedimientos o métodos desarrollados en la etapa de planificación. Por consecuente, es indispensable llevar el registro de las mediciones de acuerdo con los formatos

diseñados en esta etapa, los mismos que son Importantees para el monitoreo y comprobación de la ruta de las acciones.

Verificar los procesos y los Resultados obtenidos

Los datos obtenidos en la etapa anterior deben ser verificados mediante herramientas estadísticas y gráficas que comprueben que el proceso esté dentro de los límites especificados. Dichos Resultados deben ser comunicados a todas las áreas y personal implicado lo más pronto posible, para que se encuentren las causas de las no conformidades y se puedan excluir o minimizar sus causas.

Tomar las acciones adecuadas

Existen tres subciclos dentro del ciclo de control empleados dependiendo de las conclusiones.

- ***Subciclo de mantenimiento:*** los Resultados son conformes, dentro del los límites establecidos en las metas (indicadores), especificaciones, procedimientos, normas.

- ***Subciclo de mejoramiento:*** existen propuestas o ideas que permiten reemplazar un estado de cosas por otro mejor. Se prueba la efectividad de las ideas para luego suscribir especificaciones o normas con niveles de desempeño superiores.

- ***Subciclo de correción:*** los Resultados no son conformes con los requisitos y se aplican correcciones inmediatas (producto de la improvisación o del oficio del personal) las cuales influyen lo más pronto posible en los Resultados.

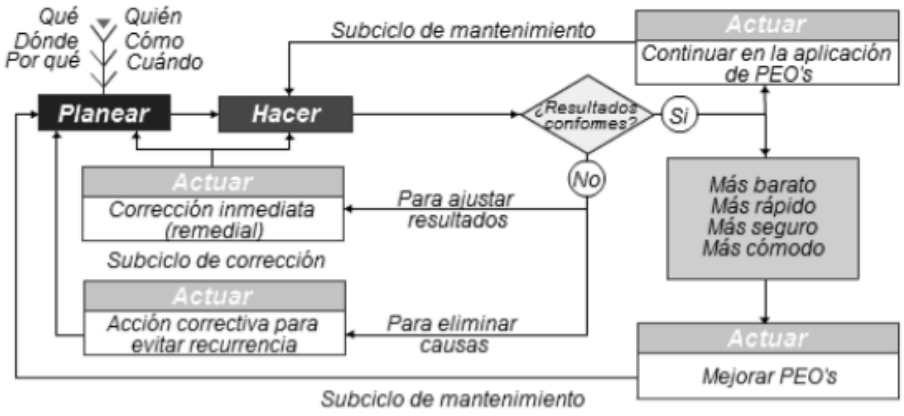


FIGURA 2.6: Subciclos de la toma de decisiones. Tomado De Universidad Tecvirtual Del Sistemas Tecnológico De Monterrey (Mexico, 2012)

2.2.2. ISO /IEC 27001

Este sistema permite disminuir los riesgos y protege la información de los procesos de las empresas, esta normativa se enfoca a un sistema de gestión de seguridad de información.

2.2.3. Diagrama de flujo BPMN

Describe los estándares business process modeler notation, y los procesos basados en el sistema de gestión de procesos SGP. Cumpliendo las siguientes características:

- Utiliza lenguaje grafico común.
- Funciones integradas.
- Es adaptable a los cambios.
- Optimiza los procesos.

2.2.4. Gestión de proyectos – PMBOK

La guía de los fundamentos para la dirección de proyectos, o PMBOK por sus siglas en inglés, son un conjunto de buenas prácticas y conocimientos de los profesionales dedicados de la rama de dirección de proyectos.

Los procesos que agrupa el PMBOK son: inicio, planificación, ejecución, seguimiento y control, y cierre.

2.3. Metodología de análisis y gestión de riesgo

Para el análisis de este capítulo se utilizó metodología de gestión de proyectos PMBOX y como metodología de gestión de riesgo MARGERIT.

2.3.1. Metodología de gestión del proyecto

Esta metodología es la encontrada en PMBOX adaptada a la Gobernación de la provincia del Guayas para el proceso detallado en capítulos anteriores:

a) Iniciación:

- Levantar Requisitos del proceso de Concursos de méritos y oposición.
- Alternativas de solución.
- Aclarar los objetivos del proyecto.
- Elegir director de proyecto y equipo de Proyecto.

Se realizó el acta de la constitución del proyecto Anexado.

b) Planificación del proyecto:

- Definición de alcance.
- Estructura de desglose de trabajo.
- Cronograma del proyecto.
- Planificación de recursos humano (Organigrama).
- Estimación de costes.
- Identificación de riesgos de proyecto.
- Planificación de la respuesta a los riesgos del proyecto.

c) Ejecución del proyecto:

- Gestionar la ejecución del proyecto.
- Selección de proveedores.

d) Seguimiento y control:

- Seguimiento a las actividades programadas.
- Control de cambios.
- Cierre del proyecto.

2.3.2. Metodología para el diseño e implementación de un SGSI

Metodología de MARGERIT que se detalla a continuación:

a) Política de SGSI:

- Marco Referencial de los objetivos.

- Requerimientos que se necesitan en el proceso de concurso de méritos y oposición.
- Criterio de evaluación de riesgo.

b) Manual del SGSI:

- Definir alcances aplicables.
- Definir responsables de ejecución y cumplimiento.

c) Análisis de brechas:

- Generalidades.
- Seguridad lógica.
- Seguridad personal.
- Seguridad física ambiental.
- Inventario de activos y clasificación de la información.
- Administración de las operaciones y comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas informático.
- Procesamientos de respaldos.
- Gestión de incidentes de seguridad de información.

d) Análisis y evaluación de riesgos:

- Identificación de procesos (Diagrama de proceso).

- Identificación de activos (método de la elipse).
- Inventario de activos.
- Análisis y evaluación de riesgos.

Análisis de riegos:

Es el estudio de las posibles amenazas y vulnerabilidades a los que están expuestos los recursos y servicios que ofrece TI a la organización u que permite estimar la magnitud de los impactos que pueda ocasionar a la organización en caso de producirse los riesgos.

Acciones a realizar en un análisis de riesgos:

1. Determinar el alcance del análisis de riesgo de TI.
2. Identificar todos los activos de información de la organización, su interrelación y su valor, en el sentido de que perjuicio (coste) supondría su degradación.
3. Identificar las principales amenazas de los activos de la información.
4. Identificar las principales vulnerabilidades que pueden generar las amenazas de cada activo de información.
5. Identificar la probabilidad que tienen cada una de las vulnerabilidades identificadas.

6. Con estos elementos se puede estimar:
    a. El impacto: lo que podría pasar y el análisis CID.
    b. El riesgo: lo que probablemente pase.
7. Desarrollo de la matriz de riesgo.
8. Interpretación de la matriz de riesgo, conclusiones y recomendaciones.

2.4. Estadística actual

Según el reporte "Internet Security Threat Report" (Symantec, 2017) publicado por Symantec en abril de 2017 indica que las páginas web escaneadas con vulnerabilidades, las cuales, si son explotadas, pueden permitir ejecutar código malicioso sin la interacción del usuario, Resultadoando potencialmente una fuga de información para luego comprometer a los visitantes de los sitios afectados, ha disminuido un 2% con relación al año 2015. Mientras que el porcentaje de vulnerabilidades consideradas criticas representa un 6% menos con relación al mismo año.

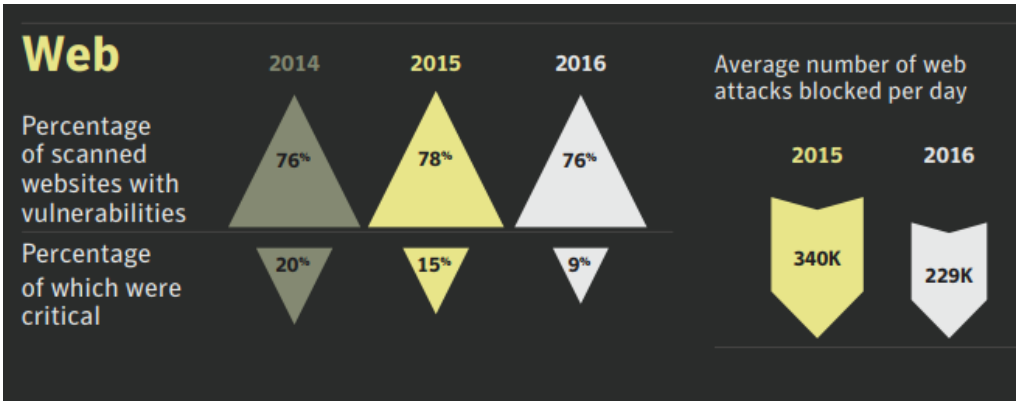


FIGURA 2.7: Páginas escaneadas con vulnerabilidades. symantec corporation (april, 2016) istr 2017. Recuperado De https://www.symantec.com/security-center/threat-report

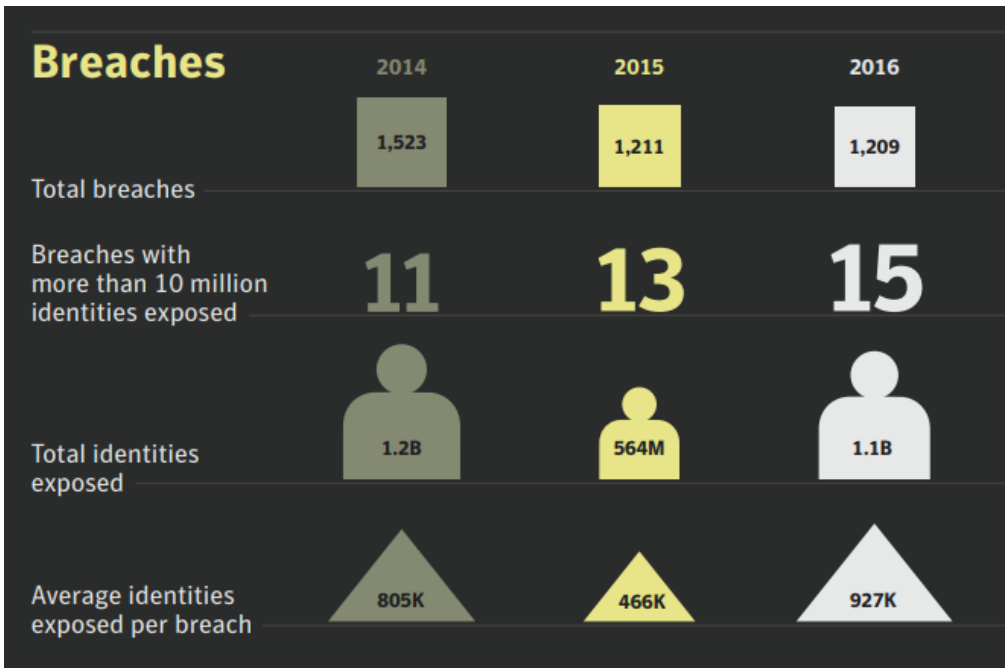


FIGURA 2.8: Brechas. Symantec Corporation (April, 2016) Istr 2017. Recuperado De https://www.symantec.com/security-center/threat-report

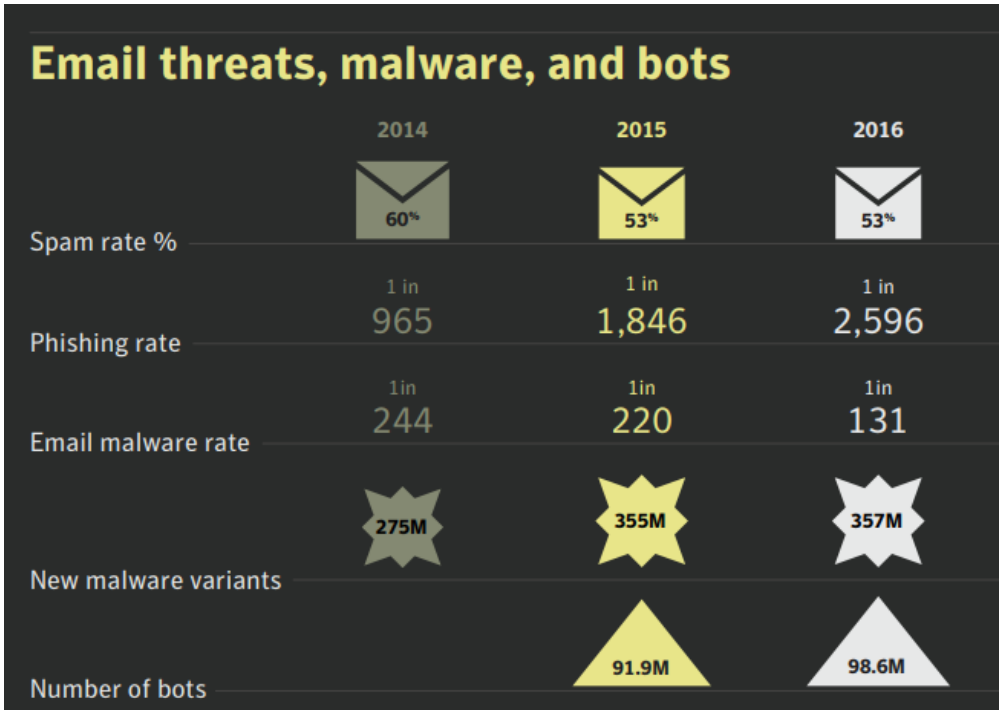


FIGURA 2.9: Amenazas De Email, Malware Y Bots. Symantec Corporation (April, 2016) ISTR 2017. Recuperado De https://www.symantec.com/security-center/threat-report

CAPÍTULO 3

ANÁLISIS DE LA UNIDAD DE TALENTO HUMANO

3.1. Situación actual

Debido a la necesidad de implementar un SGSI Cumpliendo la Normativa ISO 27001 para la Gobernación de la Provincia del Guayas en el proceso de Concurso de méritos y oposiciones, se procede a realizar un diagnóstico de la situación actual ya que la institución no cuenta con un Sistema de Seguridad de la información.

Se inicia el proceso desde la planificación de concurso de mérito y oposición y culmina con la expedición del nombramiento provisional de prueba por parte de la autoridad nominadora o el delegado.

UATH debe aplicar las normas técnicas del subsistema de selección del personal el cual se preocupa por lo siguiente: La planificación que debe ser restructurada de acuerdo a las necesidades, capacidad técnica y financiera. La igualdad de trato sin distinción alguna de los deberes y derechos de los postulantes. La transparencia ya que la información debe ser accesible a cualquier ciudadano a través de la plataforma. El control técnico y profesionalismo de los administradores del proceso. La confidencialidad ya que tiene información de índole personal de los postulantes, así como la documentación de reserva necesaria para ejecución del proceso detallados en el artículo 3 del ministerial no. MDT-2015-0046, publicado en el registro oficial no. 467, de 26 de marzo de 2005.

3.1.1. Responsables del proceso de concurso de mérito y oposición de la Gobernación del Guayas

De acuerdo al artículo 8 del acuerdo ministerial 222 del registro oficial suplemento 383 del 26 de noviembre del 2014 con su última

modificación 24 de abril del 2015. Detalla que los responsables de concurso del mérito y oposición son:

- Unidad administrativa de talento humano:
    - Responsable de la unidad.
    - Encargada de administración del concurso.

- Tribunal de mérito y oposiciones:
    - Autoridad nominadora o delegado.
    - Responsable de la UATH o delegado.
    - Responsable de la unidad administrativa del puesto vacante.

- Tribunal de apelaciones:
    - Autoridad nominadora o delegado.
    - Responsable de la UATH o delegado.
    - Responsable de la unidad administrativa del puesto vacante.

3.1.2. Descripción de los Flujos y detalle del proceso

El proceso de concurso de méritos y oposición contiene 5 procesos con sus respectivos subprocesos, que se detalla a continuación en el diagrama de Flujo BPMN.

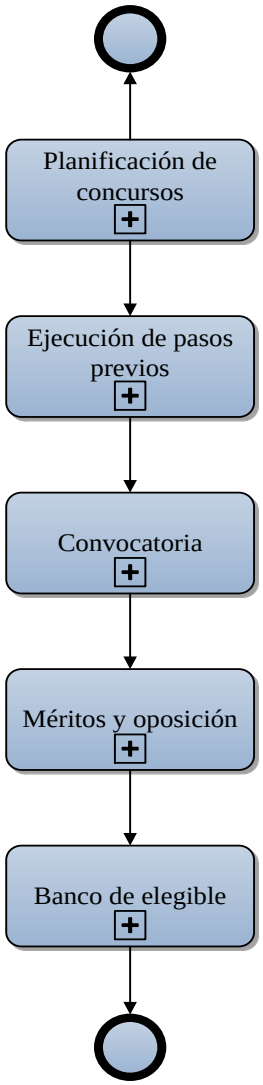


FIGURA 3.10: Flujo De Concurso De Meritos Y Oposiciones.

Fuente: Los Autores

3.1.2.1. Subproceso de Planificación de concurso

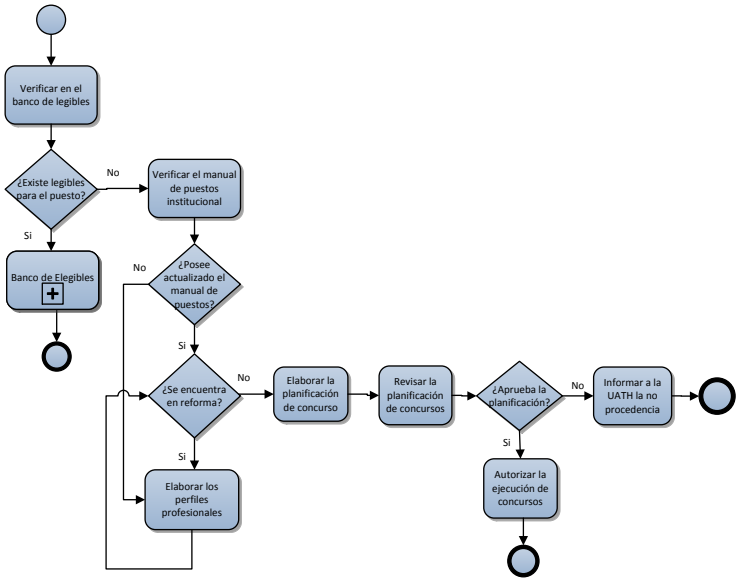


FIGURA 3.11: Flujo de subproceso de planificación de concurso. Fuente: Los autores

- **Verificar en el banco de elegibles:** Antes de iniciar con la planificación de concursos el responsable de UATH debe revisar si existe un banco elegible para cubrir la vacante solicitada.

- **Verificar el manual de puestos institucionales:** Se debe comprobar que los puestos solicitados para los concursos de méritos y oposición están en el manual, si no están se debe crearlo según los perfiles necesarios.

- **Elaborar los perfiles provisionales:** Se debe analizar el perfil provisional, luego solicitar la aprobación al ministerio de trabajo, adjuntando el informe técnico respectivo donde se detalla la necesidad. Una vez aprobado se continúa al otro proceso.

- **Elaborar la planificación de concursos:** Se debe analizar los puestos vacantes y la creación de puestos contemplados en la planificación de talento humano. Se debe usar el banco legible si es que existe, si no al realizar el proceso de banco legible, se genera los memorandos para revisión por parte de la autoridad nominadora.

- **Revisar la planificación de concursos:** Se revisa por la autoridad nominadora o su delegado para su aprobación o negación considerando los parámetros detallados a continuación:
    - Fechas en la programación.
    - Reclasificación de partidas.
    - Procesos de restructuración.

- **Informar a la UATH la no procedencia:** Si la planificación no fue aprobada por la autoridad nominadora se debe realizar los informes técnicos y memorando

- **Autorizar la ejecución de concursos:** Previa a la ejecución de los concursos la autoridad nominadora aprueba en un memorando emitido por UATH.

3.1.2.2. Subproceso de ejecución de pasos previos

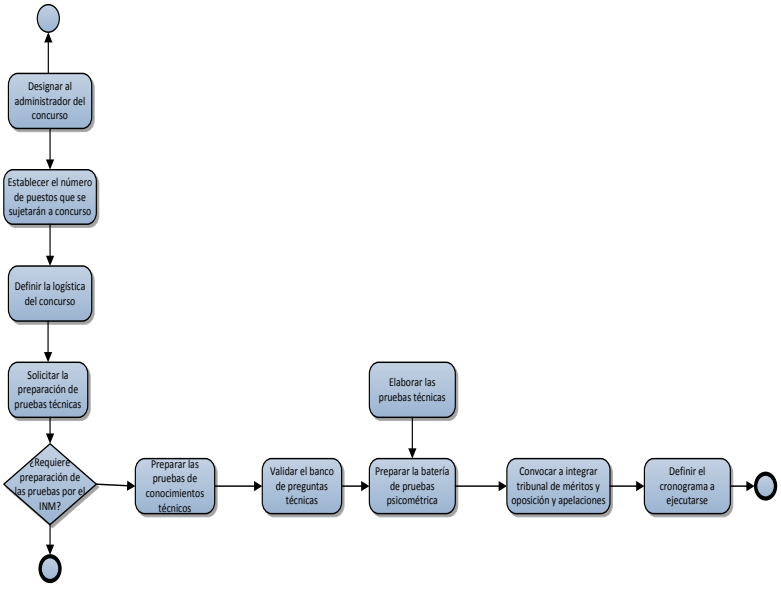


FIGURA 3.12: Flujo de subproceso de ejecución de pasos previos. Fuente Los Autores

- **Designación al administrador del concurso:** Se delega de parte de UATH un administrador quien será el encargado de todo el proceso de selección.

- **Establecer el número de puestos que se sujetaran a concurso:** De acuerdo al numeral 2 del art. 13 de la norma técnica se validan los puesto que van a concurso, se detalla y analiza los puestos vacantes financieras, puestos vacantes comprobados, puestos vacantes sin litigio.

- **Definir la logística del concurso:** Tomar en cuenta las consideraciones para la pruebas técnicas, psicométricas y entrevistas, definiendo lugar, infraestructura, logística para lo cual se debe tomar en cuenta las siguientes consideraciones análisis de oferta y análisis de postulantes en el exterior.

- **Solicitar la preparación de pruebas técnicas:** Se solicita a la unidad que pertenece el puesto a concurso que elabore las preguntas para la prueba técnica.

- **Preparar las pruebas de conocimiento técnicos:** Para la creación de las pruebas se debe de considerar el banco de preguntas por lo menos de 100 preguntas por el puesto a concurso deben ser de opción múltiples y preguntas cerradas, las pruebas deberán ser consideradas con relación del trabajo real. Simulación del trabajo y ejercicios de análisis.

- **Validar el banco de preguntas técnicas:** El administrador de concurso debe revisar el banco de preguntas entregado, si considera cargos debe solicitar que se realice caso contrario siguen al siguiente subproceso.

- **Elaborar las pruebas técnicas:** El administrador del concurso le solita a responsable de UATH que preparen las pruebas.

- **Preparar las baterías de pruebas psicométricas**: Determinar que batería de pruebas psicométricas va

aplicar, elaborar el informe técnico y carga de la información técnica a la plataforma.

- **Convocar a integrar tribunales de méritos y oposición y apelaciones:** Se debe seguir los siguientes pasos: Convocatoria, sesión y acta

- **Definir el cronograma a ejecutarse:** Se debe seguir los siguientes pasos: confirmar la capacidad operativa UATH, registro del cronograma en la plataforma tecnológica. Siguiendo los criterios del tiempo máximo, flexibilidad, extensión del cronograma y ajustes del cronograma.

3.1.2.3. Subproceso de convocatoria

FIGURA 3.13: Flujo de subproceso de convocatoria. Fuente Los Autores

- **Publicar y difundir la convocatoria:** Se utiliza la plataforma tecnológica para hacer conocer a la comunidad de la existencia del concurso con el fin de tener gran número de postulantes, la difusión dura 4 días. Se debe publicar en la plataforma y en la página web.

- **Realizar la postulación:** Siguiendo los criterios como el que solo se puede realizar por la plataforma tecnológica, es responsabilidad

exclusiva del postulante, una vez realizada la postulación no podrá retirarse del concurso, la información publicada por el postulante en la plataforma debe ser verídica y documentada, no se toma en cuenta la información que el postulante no publicó, el postulante es el único responsable del monitoreo del concurso.

3.1.2.4. Subproceso de Mérito y oposición

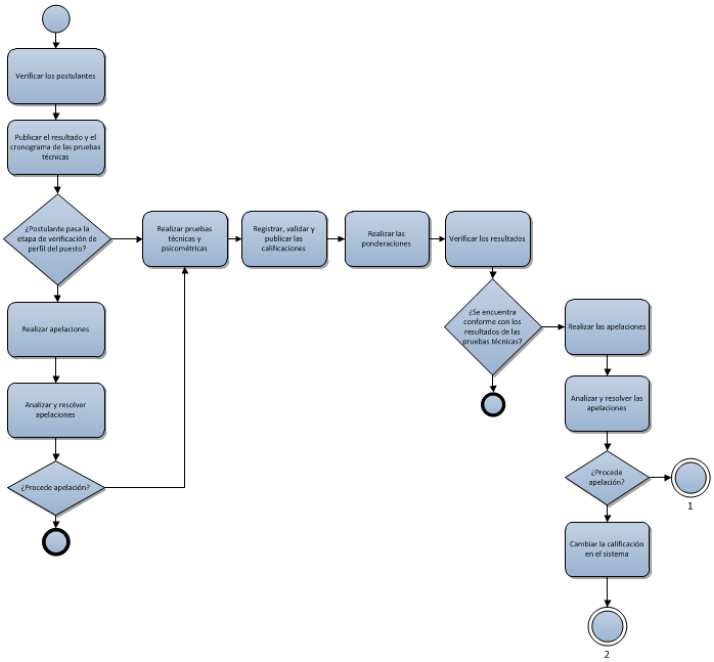


FIGURA 3.14: Flujo 1 del subproceso de méritos y posición. Fuente: los autores

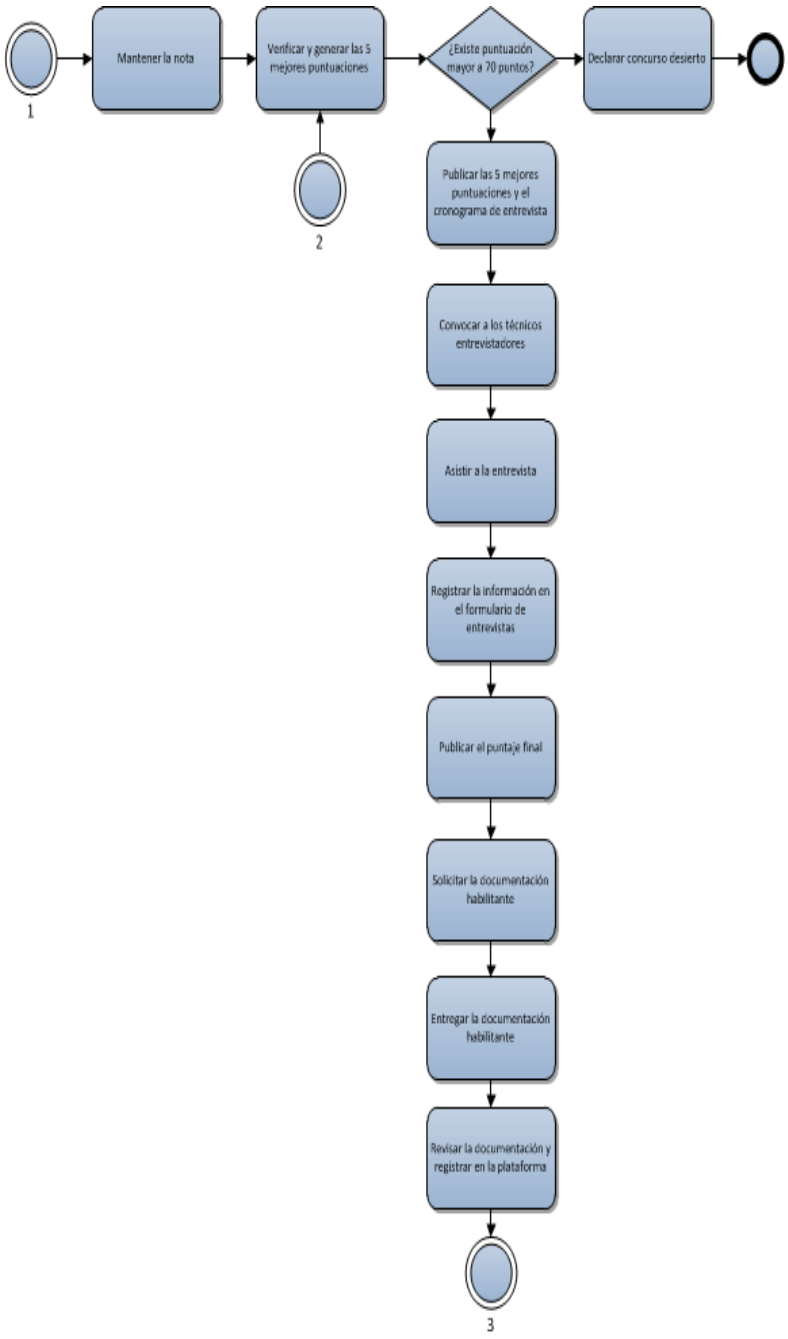


FIGURA 3.15: Flujo 2 del subproceso de méritos y posición. Fuente: los autores

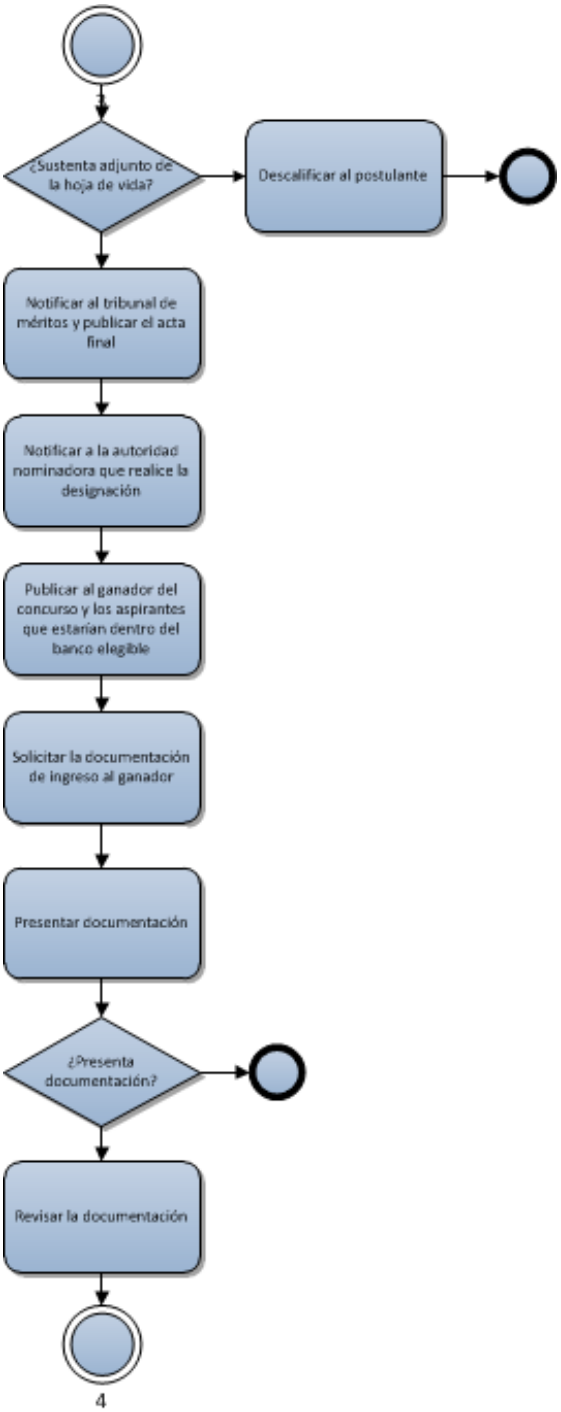


FIGURA 3.16: Flujo 3 del subproceso de méritos y posición. Fuente: Los autores

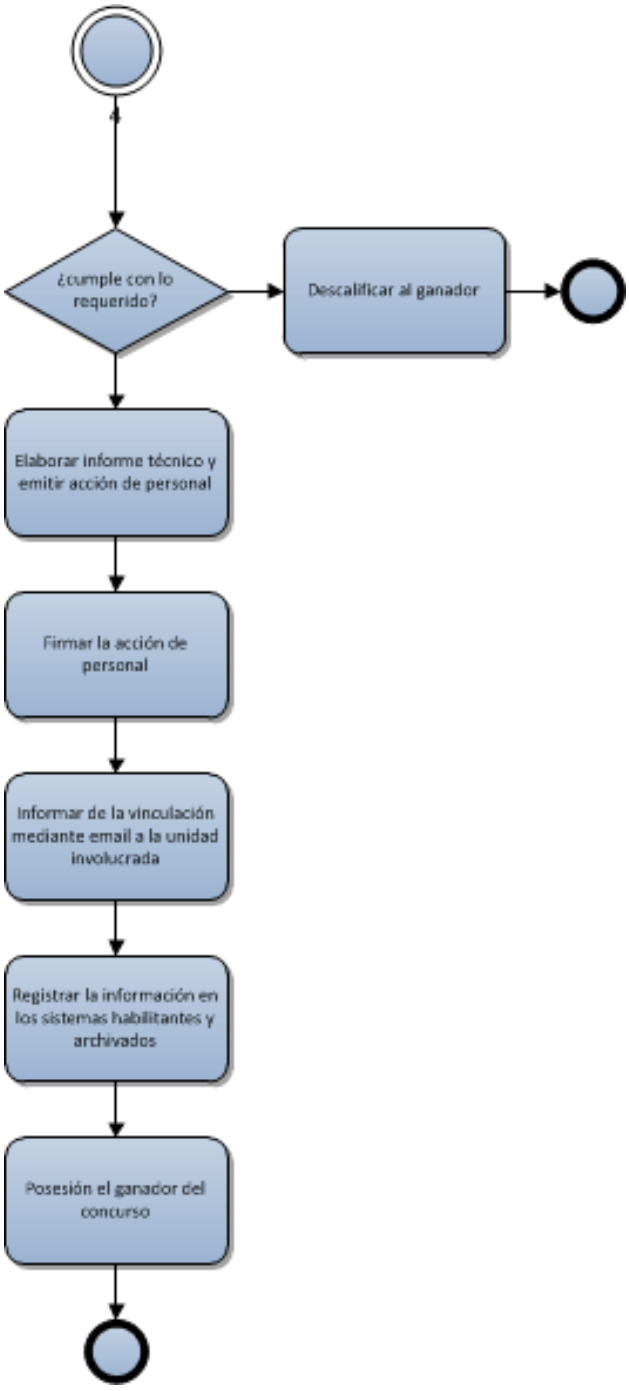


FIGURA 3.17: Flujo 4 del subproceso de méritos y posición. Fuente: Los autores

- **Verificar y publicar las postulaciones:** Se evalúa el cumplimiento del perfil del puesto a cada postulante de acuerdo a la información registrada en la plataforma. Tomando en cuenta 3 puntos para la intuición formal y 1 punto por cada año de experiencia laboral.

- **Publicar el Resultados y el cronograma de las pruebas técnicas:** Se sube a la plataforma a los postulantes con la respectiva observación de que, si cumple o no con el perfil establecido, si no cumple se coloca "NO PASA A LA SIGUIENTE ETAPA".

- **Realizar apelaciones:** El postulante q no esté de acuerdo con la calificación del mérito puede apelar. La apelación es a nivel personal.

- **Analizar y resolver apelaciones:** Se resuelve por el tribunal de apelación la cual debe ser motivado y consignado en el acta de resolución de apelación a la verificación del mérito.

- **Realizar pruebas técnicas y psicométricas:** Los postulantes deben llevar consigo su documento original de identificación. Si hay un gran número de postulantes se realizará grupos para rendir los exámenes.

- **Registrar, validar y publicar las calificaciones:** Se ingresa los Resultados manualmente al sistema, siendo responsabilidad del administrador del concurso.
- **Realizar las ponderaciones:** La calificación es 75% pruebas Técnicas y pruebas psicométricas y 25% la prueba psicométrica y debe cumplir como mínimo 70 para continuar a la siguiente etapa.

- **Verificar los Resultados:** Cada postulante tiene la obligación de monitorear las calificaciones en el sistema, si no está conforme puede apelar caso contrario se sigue con el proceso de selección.

- **Realizar las apelaciones:** Siguiendo la fecha establecida por el cronograma el postulante puede

apelar a una o varias preguntas que serán revisadas por el tribunal de apelación.

- **Analizar y resolver las apelaciones:** Los Resultados se colocarán en el acta resolutiva que será firmada por el tribunal de apelación y entregada a la UATH.

- **Mantener la nota:** Si la apelación no fue favorable el tribunal de apelación mantendrá la nota en el acta resolutiva.

- **Cambiar las calificaciones en el sistema:** Si fue favorable la apelación se modificará la calificación y se registrará el cambio en la plataforma.

- **Verificar y generar las 5 mejores puntuaciones y el cronograma de entrevistas:** Los postulantes que obtuvieron más de 70 en la calificación y corresponda a las 5 mejores notas, pasará a la fase de entrevista.

- **Declarar concurso desierto:** Si no existe postulantes con calificación mayor a 70 se da por finalizado el proceso.

- **Publicar 5 mejores puntuados y el cronograma de entrevista:** Se publica en la plataforma los 5 mejores puntuados, junto con el cronograma de entrevistas que debe ser publicado en la plataforma como en la página web.

- **Convocar a los técnicos entrevistadores:** Se conforma de 1 delegado de la unidad requirente y 1 delegado de la UATH.

- **Asistir a la entrevista:** El postulante debe asistir a la entrevista a la hora lugar y fecha destinada si no asiste será descalificado.

- **Registrar la información de formulario en el sistema:** Se sube la calificación al sistema el cual realiza los cálculos respectivos para dar el Resultados final del ganador.

- **Publicar el puntaje final:** Se genera en la plataforma el informe de reporte de puntaje final para conocimiento de los postulantes.

- **Solicitar la documentación habilitante:** Los delegados de UATH solicitan a los 5 mejor postulantes los documentos habilitantes que sustente lo que pusieron en la plataforma.

- **Entregar la documentación habilitante:** Puede ser entregados en Físico o digital al funcionario responsable de la UATH.

- **Revisar la documentación y registrar en la plataforma:** Se revisa la hoja de vida en el sistema de socio empleo y se compara con la documentación entregada.

- **Descalificar al postulante: S**i el postulante no tiene como sustentar lo ingresado en socio empleo queda descalificado y finaliza el proceso para ese postulante.

- **Notificar al tribunal de mérito y publicar el acta final:** Se notifica al tribunal de mérito para que realice el acta final que contiene los puntajes alcanzados, la declaración del ganador del concurso y los demás postulantes que pasan al banco de elegibles.

- **Notificar a la autoridad nominadora que realice la designación:** Elaborar el informe técnico para que la autoridad nominadora en 3 días realice la designación.

- **Publicar al ganador del concurso y los aspirantes que estaría dentro del banco elegibles:** Subir a la plataforma la información del ganador de concurso y los del banco elegible e informar por correo electrónico.

- **Solicitar la documentación de ingreso al ganador:** Se solicita la documentación habilitante para el ingreso y posterior vinculación del funcionario.

- **Presentar documentación:** El postulante deberá dar la documentación para su ingreso al sector público de acuerdo a lo establecido en el ministerio de trabajo.

- **Revisar la documentación:** Verificar la documentación que respalda la información ingresada en la hoja de vida entregada por el ganador.

- **Descalificar el ganador:** si el ganador no se presenta a la institución o no acepta el nombramiento entregado o no presenta los documentos completos se descalifica y se procede a ir al banco elegible a coger un postulante.

- **Elaborar informe técnico y emitir acción de personal:** según lo establecido en el artículo 67 de la LOSEP. Se realiza los informes técnicos con el acta final y la acción de personal.

- **Firmar la acción de personal:** Se emitirá un nombramiento provisional de prueba de conformidad según lo establecido en el reglamento de la LOSEP.

- **Informar de la vinculación mediante email a las unidades involucradas:** Mediante un correo electrónico se informa el ingreso del nuevo personal al área requirente. Se debe emitir 2 días antes del ingreso del funcionario.

- **Registrar la información en los sistemas habilitantes y archivar:** La UATH debe realizar la acción de personal, la unidad de nómina ingresará la información en el sistema SPRYN, se abre expediente del servidor y se ingresa en el sistema SIITH.

- **Posesión al ganador del concurso:** El ganado debe presentarse a ocupar su puesto y proceder a firmar la respectiva acción de personal.

3.1.2.5. Subproceso de banco de elegibles

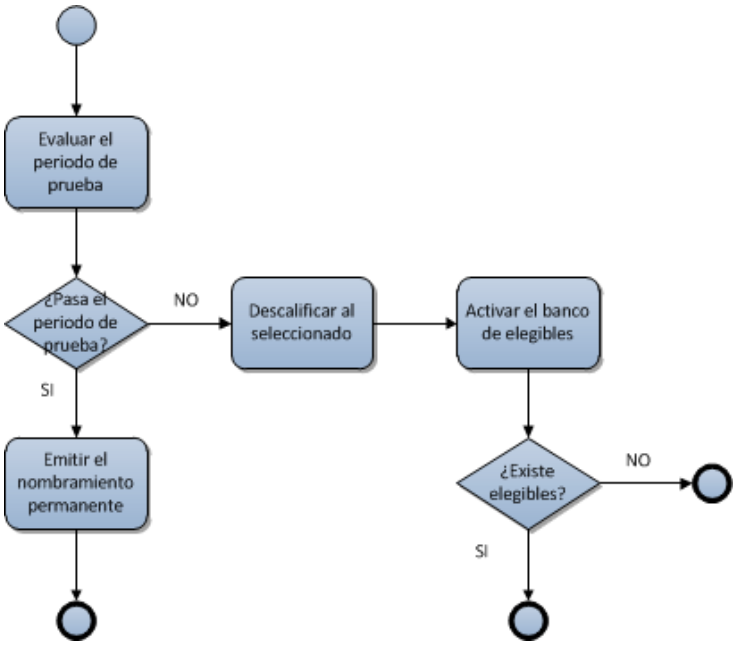


FIGURA 3.18: Flujo del subproceso de banco de elegibles. Fuente: Los autores

- **Evaluar el periodo de prueba:** El jefe inmediato evaluara los 3 meses o máximo 6 meses.

- **Emitir nombramiento permanente:** Si pasa el periodo de prueba la UATH emitirá el nombramiento permanente.
- **Descalificar el seleccionado:** En caso que no obtuviera el puntaje de prueba de 70.5% (puntaje

mínimo) la UATH procederá conforme lo dispuesto en el reglamento general de la LOSEP.

- **Activar el banco de elegibles inmediatos / potenciales elegibles:** El banco de los elegibles inmediatos se conforma de los 5 mejores puntuados excluyendo al ganador del concurso, si no existe banco elegible inmediato tenemos el potencial elegible que son los postulantes que no alcanzaron a la entrevista, pero tienen una calificación de 70 puntos o mayor a ella.

3.2. Identificación de activos de información

Un activo es aquel que tiene valor o utilidad para la Gobernación, por esta razón se necesita identificarlos para lograr la correcta operación del proceso de concursos de méritos y oposición.

FIGURA 3.19: Activos de la información. Fuente: Los autores

Para la identificación de los activos se utilizaron los datos que facilitó el responsable del área de Recursos Humanos de la Gobernación de la provincia de las guayas la Psicóloga Dennys Días, para un mejor análisis, gestión de riesgo y las decisiones que se tomen en relación con el tratamiento del riesgo se han dividido en seis categorías los activos de información:

- Activos de Gestión Documental.
- Activos de Software.
- Activos Físicos.

- Activos de Servicios.
- Activos de funcionarios.

3.2.1. Activos Gestión Documental

Soporte no electrónico que es la prueba o la acreditación de algún proceso que contiene información. Los activos de información son:

- Información electrónica:
    - Base de datos.
    - Documentos creados electrónicos.
    - Correos electrónicos.
    - Audios.
    - Videos.

- Información escrita:
    - Memorándum.
    - Oficios.
    - Actas.
    - Contratos.
    - Reglamentos.
    - Normativas.
    - Acuerdos ministeriales.

- Manual de procedimientos.

- Información hablada:
  - Conversaciones presenciales.
  - Conversaciones telefónicas.
  - Exposiciones.
  - Presentaciones virtuales (Video conferencia).

3.2.2. Activo Software

Este literal comprende de todos los programas de cómputo que incluye datos o procedimientos que se manejan en el área de Recursos Humanos que permite realizar tareas del departamento. Dependiendo de un sistema operativo. Los activos de información son:

- Software Sistema operativo:
  - Linux Centos 4.2.
  - Windows server 2003 entreprise Edition.
  - Windows 7.

- Software herramientas utilitarias:
  - Microsoft Office 2017.
  - Adobe PDF.

- Nitro Pro 8.
- Evaluar.
- Quipux.
- Zimbra.
- Socioempleo.

- Software protección:
  - Eset Nod32.
  - Malwarebytes.

- Software de administración de base de datos:
  - MySQL.

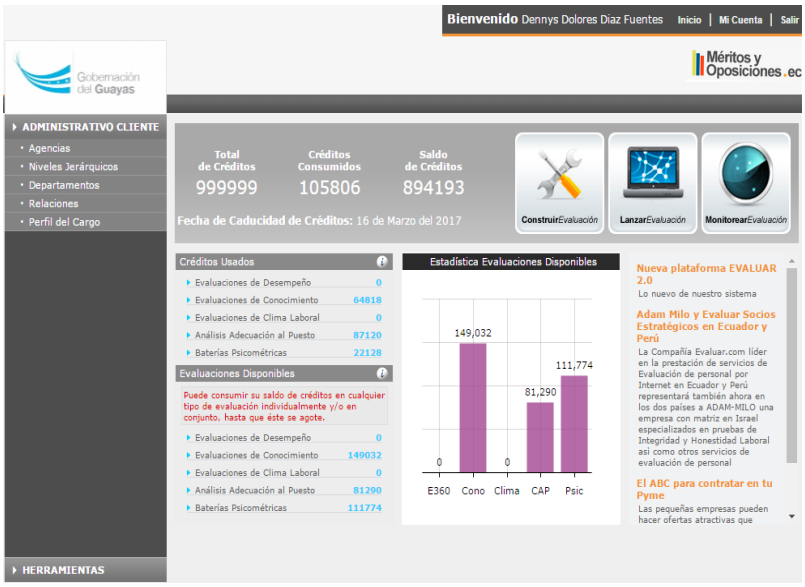


FIGURA 3.20: Sistemas de méritos y oposición. Fuente: página de la Gobernación del Guayas

3.2.3. Activos fijos

Se refiere a todos los equipos que sirven para el manejo de la información y de la comunicación en los procesos que se realiza en este departamento. Los activos de la información son:

- Hardware de procesamiento:
    - Portátiles.
    - PC´s de oficina.
    - Servidor de base de Datos.
    - Servidor de Correo Electrónico.
    - Servidor de respaldo.
    - Servidor de Dominio.
    - Servidor de IAS (Internet Access Server).

- Hardware de comunicación:
    - Routers.
    - Central digital.
    - Fax.
    - Teléfono IP.
    - Switches.
    - Cableado estructurado.
    - Tecnología Ethernet.

- Hardware de almacenamiento:
    - Discos duro externos.
    - CD´s.
    - DVD’s.
    - Memorias USB.

- Mobiliario y equipamiento:
    - Archivadores.

- Equipos de oficina:
    - Scanner.
    - Impresora.
    - Copiadora.

3.2.4. Activos de Servicios

Todas las funciones brindadas ya sean por una persona natural o por una empresa con la finalidad de que satisfaga con la necesidad solicitada. Los activos de la información son:

- Comunicación:
    - Central Telefónica.
    - Correo electrónico.

- Hosting y Pagina web.

- Servicio general:
  - Red eléctrica.

- Servicios de Concurso de méritos y oposición:
  - Sistemas contratados para evaluar los concursos (Evaluar).

3.2.5. Activos de funcionarios

Son las personas que intervienen en la manipulación de la información en sus actividades y que tienen una responsabilidad específica sobre los subprocesos que se realizan. Por lo tanto, Disponen de privilegios particulares para accesos al sistema de información para cumplir con sus actividades cotidianas. Los activos de la información son:

- Jefa de Recursos humano (Responsable de la UATH).
- Delegado al tribunal de Méritos y oposición.
- Responsable de la unidad Administrativa de la vacante del puesto.
- Analista 2 de Recursos Humanos (Administrador del Concurso).

- Analista 1 de Recursos Humanos (Administrador de SocioEmpleo).
- Servidor público de apoyo 4 (Responsable de Secretaría).

3.3. Valoración de los activos

La valoración nos ayuda a determinar el impacto que puede sufrir la Gobernación de la provincia de las guayas por la pérdida de la confidencialidad, integridad y disponibilidad. Esta valoración se realizó con ayuda de la unidad administrativa de talento humano y el departamento de tecnología de la comunicación y la información que son los que conocen el proceso de mérito y oposición y la importancia que cada activo tiene.

La escala que se utiliza para el análisis de la valoración de los activos son los detallados en los 3 cuadros siguientes:

TABLA 4: Tabla de clase de activos para confidencialidad

Activos de información (Confidencialidad)	Clase	Descripción
1	Pública	Puede ser visto por

		personas externas de la institución
2	Uno interno	Puede ser visto por usuarios de la Gobernación del Guayas
3	Secreto	Puede ser visto solo para el personal autorizado al proceso de concurso
4	Alta confidencialidad	Puede solo ser visto solo a personal específico

Datos obtenidos en el campo (Elaboración propia)

TABLA 5: Tabla de clase de activos para integridad

Activos de información (Integridad)	Clase	Descripción
1	No necesaria	No tiene problema si consulta la información
2	Necesaria	Hay problemas, pero no afecta el proceso
3	Importante	Hay un efecto fatal en las operaciones

Datos obtenidos en el campo (Elaboración propia)

TABLA 6: Tabla de clase de activos para disponibilidad

Activos de información (Disponibilidad)	Clase	Descripción
1	Bajo	Si no está disponible la información cuando es necesaria, no causa efectos
2	Medio	Si no está disponible la información cuando no es necesario se demora el proceso hasta que se suba la información
3	Alto	Si no está disponible la información cuando no es necesario causaría un fatal efecto en las operaciones

Datos obtenidos en el campo (Elaboración propia)

Para valorar el riesgo de los activos de acuerdo con la necesidad de la Gobernación de las guayas, basándonos en los tres elementos Confidencialidad, integridad, disponibilidad. Explicará en los cuadros a continuación:

TABLA 7: Tabla de valor de los activos

Activo	Elementos De Información	Valor	Razón
Información electrónica	Confidencialidad	3	Solo debe ser visto por personas autorizadas
	Integridad	3	Es de suma importancia que la información no se alterada
	Disponibilidad	2	Que se accese a la información en cualquier momento que se requiera
Información escrita	Confidencialidad	3	Solo debe ser visto por personas autorizadas
	Integridad	3	Es de suma importancia que la información no se alterada, ni que se

			pierda porque son documentos del estado
	Disponibilidad	2	Que se accese a la información en cualquier momento que se requiera
Información hablada	Confidencialidad	3	Solo se puede dialogar de temas privados que involucre al participante entre personas autorizadas
	Integridad	3	Es de suma importancia que la información no se filtre o se dialogue a terceros que no tienen autorización a conocer temas privados del

			concurso
	Disponibilidad	2	Que se pueda comunicar en cualquier instante de novedades del concurso
Sistema operativo	Confidencialidad	4	Se encuentra la información en el servidor por lo que debe ser protegida esta información
	Integridad	3	Los datos que se encuentran en el sistema operativo deben ser correcto
	Disponibilidad	3	La continuidad exitosa del sistema operativa es fundamental para el proceso
Software herramientas	Confidencialidad	2	Puede ser usado por cualquier personal

utilitarias			de la gobernación y no causaría efecto
	Integridad	1	Es necesaria pero no afecta el proceso q use otras herramientas utilitarias
	Disponibilidad	2	Debe ser utilizado continuamente a cualquier hora pero sin embargo puede usar otro equipo que tenga el mismo software.
Software protección	Confidencialidad	4	Solo debe ser utilizado por el personal autorizado para mantener la seguridad de la información
	Integridad	3	Si llega a fallar hay efectos fuertes en

			las operaciones
	Disponibilidad	3	el software de protección siempre debe estar disponible
Software de administración de base de datos	Confidencialidad	4	Es de alta confidencialidad porque se maneja información de los concursantes
	Integridad	3	Debe mantener integridad para que no exista modificaciones en la información de los participantes
	Disponibilidad	3	La base de datos siempre debe estar disponible
Hardware de procesamiento	Confidencialidad	4	Solo personal especializado debe ingresar a esta

			información y con la autorización respectivas para que no pueda ser modificada
	Integridad	3	Hay que asegurarse que la información no sea modificada ni alterada para que no perjudique la seriedad del concurso
	Disponibilidad	3	Debe estar 100% activo para no afectar el proceso del concurso
Hardware de comunicación	Confidencialidad	4	Solo personal especializado debe ingresar a esta información y con la autorización respectivas para que

			no pueda ser modificada
	Integridad	4	Hay que asegurarse que la información no sea modificada ni alterada para que no perjudique la seriedad del concurso
	Disponibilidad	4	Debe estar 100% activo para no afectar el proceso del concurso
Hardware de almacenamiento	Confidencialidad	4	Solo personal especializado debe ingresar a esta información y con la autorización respectivas para que no pueda ser modificada
	Integridad	4	Hay que asegurarse

			que la información no sea modificada ni alterada para que no perjudique la seriedad del concurso
	Disponibilidad	4	Debe estar 100% activo para no afectar el proceso del concurso
Mobiliario y equipamiento	Confidencialidad	1	Es los equipos públicos a utilizarse por los funcionarios
	Integridad	3	Se debe proteger la integridad física de los mobiliarios y equipos que ayudan a realizar los procesos
	Disponibilidad	1	Si no utilizan los mobiliarios y equipos igual se puede

			realizar por web de otro lado con otros equipos
Equipos de oficina	Confidencialidad	3	La información del equipo puede ser utilizada y visualizada por la persona autorizada.
	Integridad	3	Es Importantee la integridad de la información almacenada sobre todo si tiene información de los postulantes al concurso.
	Disponibilidad	2	Para que el funcionario pueda realizar el proceso tiene que accesar a la información, pero igual puede

			obtenerla el sitio web desde cualquier equipo.
Comunicación	Confidencialidad	2	Se debe proteger las líneas que no sean interceptada por terceros
	Integridad	2	Deben funcionar adecuadamente
	Disponibilidad	2	Se requiere que esté disponible pero igual no afecta mucho al proceso de concurso
Servicio general	Confidencialidad	1	Los servicios generales no requieren confidencialidad
	Integridad	2	Los servicios generales no deben sufrir manipulación
	Disponibilidad	3	Debe estar funcionando a su

			totalidad para no interrumpir los procesos
Servicios de Concurso de méritos y oposición	Confidencialidad	4	Alta confidencialidad porque usa la información de los participantes de los procesos del concurso
	Integridad	3	Debe mantener la integridad ya que no debe sufrir modificaciones de los participantes
	Disponibilidad	3	Debe estar disponible 24 / 7 la información de los concursos
Jefa de Recursos humano (Responsable	Confidencialidad	4	La información debe ser manejada dentro de la Gobernación la cual no debe ser

de la UATH)			divulgada
	Integridad	1	No se relaciona con la integridad
	Disponibilidad	3	Deben estar disponible para problema que se presente
Delegado al tribunal de Méritos y oposición	Confidencialidad	4	La información debe ser manejada dentro de la Gobernación la cual no debe ser divulgada
	Integridad	1	No se relaciona con la integridad
	Disponibilidad	3	Deben estar disponible para problema que se presente
Responsable de la unidad Administrativa de la vacante	Confidencialidad	4	La información debe ser manejada dentro de la Gobernación la cual no debe ser

del puesto			divulgada
	Integridad	1	No se relaciona con la integridad
	Disponibilidad	3	Deben estar disponible para problema que se presente
Analista 1 de recursos humano (Administrador de SocioEmpleo)	Confidencialidad	4	La información debe ser manejada dentro de la Gobernación la cual no debe ser divulgada
	Integridad	1	No se relaciona con la integridad
	Disponibilidad	3	Deben estar disponible para problema que se presente
Analista 2 de Recursos Humanos (Administrador	Confidencialidad	4	La información debe ser manejada dentro de la Gobernación la cual no debe ser

del Concurso)			divulgada
	Integridad	1	No se relaciona con la integridad
	Disponibilidad	3	Deben estar disponible para problema que se presente
Servidor público de apoyo 4 (Responsable de Secretaría	Confidencialidad	4	La información debe ser manejada dentro de la Gobernación la cual no debe ser divulgada
	Integridad	1	No se relaciona con la integridad
	Disponibilidad	3	Deben estar disponible para problema que se presente

Datos obtenidos en el campo (Elaboración propia)

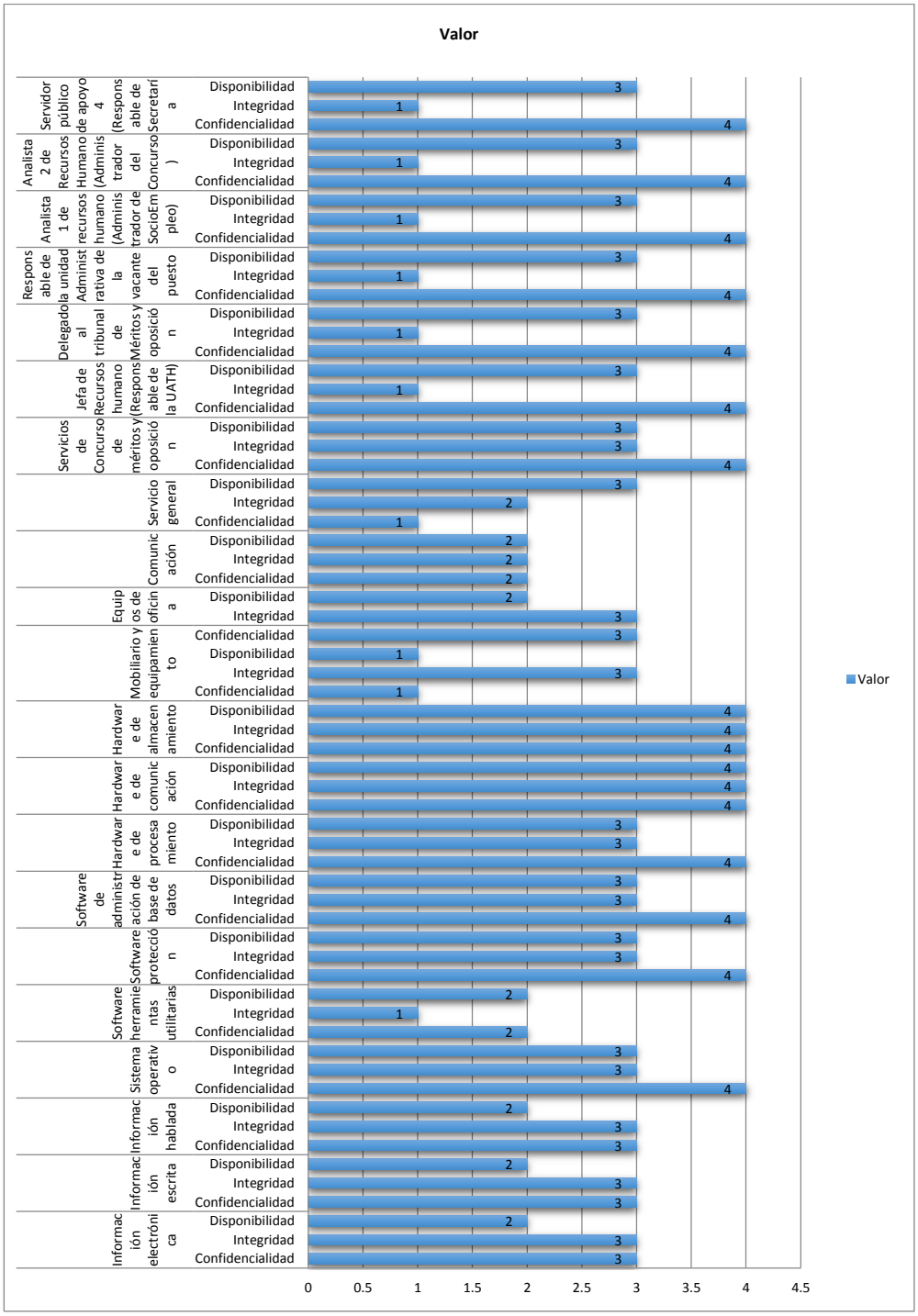


Figura 3. 21: Diagrama De Barra Del Valor De Los Activos.

Fuente: Los Autores

3.4. Definición de las amenazas y vulnerabilidades del proceso de concursos de méritos y oposición

El fin de este literal es definir las amenazas y vulnerabilidades posibles dentro de la Gobernación del Guayas dentro del proceso. Las amenazas son todo lo que puede interferir con el buen funcionamiento de los activos y las vulnerabilidades son todas las debilidades de seguridad que causa daños a las amenazas generando pérdidas y afecta a los activos.

El cuadro a continuación detalla las amenazas y vulnerabilidades que se encuentran en el proceso de concurso de méritos y oposición:

A continuación, se detalla las vulnerabilidades de los activos y las amenazas

TABLA 8: Tabla de amenazas y vulnerabilidades de los activos

Activo	Amenaza	Vulnerabilidad
Información electrónica	• Manipulación de la información • Mala conFiguración de archivos	• Métodos o protocolos usados no seguros • Firmas en los documentos electrónicos de seguridad no validadas

	• Robo de correos electrónicos • Robo de información en equipos	• Bugs no parchados en el sistema de base de datos • Contraseñas débiles en correos y equipos computacionales.
Información escrita	• Fuego • Daño por agua • Desastres naturales	• Falta de protección contra fuego • Falta de Protección física • Condición local no adecuada para desastres
Información hablada	• Manipulación de la información	• No actualización en los firmwares de equipos de videoconferencia, teléfonos
Sistema Operativo	• Mala conFiguración de archivos del sistema	• No aplicación de actualizaciones críticas al sistema operativo
Software de Herramienta Utilitaria	• Instalación de utilitarios de manera ilegal	• No uso de llaves de activación en los utilitarios instalados. • Falta de actualización para corregir errores y problemas

		de seguridad.
Software Protección	• Instalación de software de protección de manera ilegal	• Ejecución de código de fuente desconocida. • Abertura de backdoors sin conocimiento del administrador
Software de administración de la Base de Datos	• Mala conFiguración de los archivos de conFiguración de la base de datos mySQL	• No tener actualizado la base de datos con las últimas correcciones
Hardware de procesamiento	• Fuego • Daño por agua • Desastres naturales	• Falta de protección contra fuego • Falta de Protección física • Condición local no adecuada para desastres Falta de protección contra fuego
Hardware de comunicación	• Fuego • Daño por agua • Desastres naturales	• Falta de protección contra fuego • Falta de Protección física • Condición local no adecuada para desastres
Hardware de	• Fuego	• Falta de protección contra

Almacenamiento	• Daño por agua • Desastres naturales	fuego • Falta de Protección física • Condición local no adecuada para desastres
Mobiliario y equipamiento	• Fuego • Daño por agua • Desastres naturales	• Falta de protección contra fuego • Falta de Protección física • Condición local no adecuada para desastres
Equipo de Oficina	• Fuego • Daño por agua • Desastres naturales • Corte de electricidad • Degradación de Hardware • Temperatura no adecuada • Uso mal intencionado de los recursos	• Falta de protección contra fuego • Falta de Protección física • Condición local no adecuada para desastres • Falta de UPS en el edificio de la Gobernación • Falta de políticas y procedimientos de mantenimiento correctivo y preventivo • Funcionamiento deteriorado de los aires acondicionados

	• Robo • Incumplimiento de la legislación • Error de mantenimiento	• Falta de políticas de uso de equipos • Falta de protección a los suministros de equipo • falta de normas de protección de equipos • Falta de políticas y procedimientos de mantenimiento correctivo y preventivo
Comunicación	• Fuego • Daño por agua • Desastres naturales • Degradación de hardware y servicio • Errores de conFiguración • Uso mal intencionado de los recursos	• Falta de protección contra fuego • Falta de Protección física • Condición local no adecuada para desastres • Falta de políticas y procedimientos de mantenimiento correctivo y preventivo • Falta de conFiguraciones adecuadas a las necesidades • Falta de políticas
Servicio General	• Fuego	• Falta de protección contra

	• Daño por agua • Desastres naturales • Ataque Destructivos	fuego • Falta de Protección física • Condición local no adecuada para desastres Falta de protección contra fuego • Escases de protección física
Servicio de concurso de méritos y oposición	• Errores de usuarios • Errores de administración • Errores de conFiguración • Fuga de información • Alteración de información • Ingreso de información errónea	• Falta de conocimiento del uso del servicio • Falta de capacitación a los administradores • Falta de capacitación a los administradores de la plataforma • La falta de normativas sobre el uso y políticas de la información • Falta de control de cambios en la información • Falta de capacitación a los administradores de la plataforma

	• Incumplimiento de legislación • Uso mal intencionado de los recursos • Manipulación de la información • Divulgación de la información • Ingeniería social	• Falta de conocimiento en las leyes y normas de concurso por parte de los administradores • Insuficiencia en la seguridad de la información • Insuficiencia en la seguridad de la información • Insuficiencia en la seguridad de la información • Insuficiencia en la seguridad de la información
Jefe de Recursos Humanos	• Divulgación de la información • Error de usuario • Errores de administración • Incumplimiento de la	• Falta de normativas del manejo de la información • Falta de conocimiento y de capacitaciones • Falta de normativa administrativa • Falta de conocimiento de los acuerdos ministeriales

	legislación • Manipulación de la información	• Falta de normativas del manejo de la información
Delegado al tribunal de Méritos y oposición	• Divulgación de la información • Error de usuario • Incumplimiento de la legislación • Manipulación de la información	• Falta de normativas del manejo de la información • Falta de conocimiento y de capacitaciones • Falta de conocimiento de los acuerdos ministeriales • Falta de normativas del manejo de la información
Responsable de la unidad Administrativa de la vacante del puesto	• Divulgación de la información • Error de usuario • Errores de administración • Incumplimiento de la legislación	• Falta de normativas del manejo de la información • Falta de conocimiento y de capacitaciones • Falta de normativa administrativa • Falta de conocimiento de los acuerdos ministeriales

Analista 1 de recursos humano	• Divulgación de la información • Error de usuario • Incumplimiento de la legislación	• Falta de normativas del manejo de la información • Falta de conocimiento y de capacitaciones • Falta de conocimiento de los acuerdos ministeriales
Analista 2 de Recursos Humanos	• Divulgación de la información • Error de usuario • Incumplimiento de la legislación	• Falta de normativas del manejo de la información • Falta de conocimiento y de capacitaciones • Falta de conocimiento de los acuerdos ministeriales
Servidor público de apoyo 4	• Divulgación de la información • Error de usuario • Incumplimiento de la legislación	• Falta de normativas del manejo de la información • Falta de conocimiento y de capacitaciones • Falta de conocimiento de los acuerdos ministeriales

Datos obtenidos en el campo (Elaboración propia)

3.5. Análisis de riesgo

La Gobernación del Guayas está expuesta a riesgos los cuales se va a determinar por medio de este proceso sistemático. Que ayuda a determinar qué tan protegido está el sistema. Los riesgos son los daños, son aquellos eventos negativos que pone en la cuerda floja a nuestros sistemas.

Según los estándares de la ISO 27001 se determina en la siguiente Figura los procesos para la evaluación de riesgo.

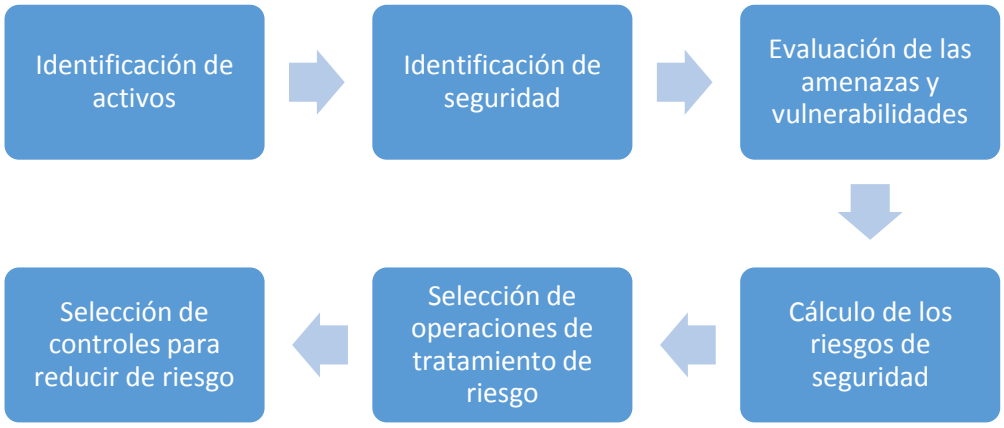


FIGURA 3.22: Análisis de riesgo ISO 27001. Fuente: Los autores

3.5.1. Determinación del Riesgo

En este literal se identifica y calcula los riesgos de los activos, cálculo de amenazas y vulnerabilidades.

3.5.1.1. Evaluación de riesgos del proyecto

TABLA 9: Valor de la probabilidad

Probabilidad	Valor
Muy Importante	1
Relativamente probable	2
Probable	3
Muy probable	4
Casi certeza	5

Datos obtenidos en el campo (Elaboración propia)

TABLA 10: Valor del impacto

Impacto	Valor
Muy bajo	1
Bajo	2
Moderado	3
Alto	4
Muy alto	5

Datos obtenidos en el campo (Elaboración propia)

TABLA 11: Probabilidad del impacto al riesgo

Tipo de riesgo	Probabilidad
Muy alto	Mayor a 49

Alto	30-49
Moderado	20-29
Bajo	10-19
Muy bajo	Menor a 10

Datos obtenidos en el campo (Elaboración propia)

3.5.1.2. Riesgos Generales

TABLA 12: Tabla de riesgos generales

Riesgo	Causa	Prob	Obj. Afec	Imp	Prob X imp	Tipo RG
RG1: Incumplimiento en el cronograma	Poca disponibilidad de los responsables	5.00	Alcance	1.00	5.00	Alto
			Tiempo	5.00	25.00	
			Costo	1.00	5.00	
			Calidad	2.00	10.00	
			Total Prob. impacto		45.00	
RG2: Actividades no programadas	Solicitud del comité de seguridad de la información	4.00	Alcance	2.00	8.00	Alto
			Tiempo	4.00	16.00	
			Costo	1.00	4.00	
			Calidad	2.00	8.00	
			Total Prob. impacto		36.00	
RG3: Modificación del	solicitud del comité de	3.00	Alcance	2.00	6.00	Moderado
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	

cronograma del proyecto	seguridad		Calidad	1.00	3.00	
			Total Prob. impacto		27.00	
RG4: Falla del personal	Vacaciones, enfermedad, permisos, entre otros	3.00	Alcance	1.00	3.00	Moderado
			Tiempo	3.00	9.00	
			Costo	2.00	6.00	
			Calidad	2.00	6.00	
			Total probabilidad por impacto		24.00	
RG5: cambios en el proceso de meritocracia	Modificación en los procesos dados por el ministerio de trabajo	4.00	Alcance	2.00	8.00	Alto
			Tiempo	5.00	20.00	
			Costo	1.00	4.00	
			Calidad	2.00	8.00	
			Total Prob. impacto		40.00	
RG6: cambio de personal base involucrado en la seguridad de la información	términos de contrato, despido, renuncia, entre otros	2.00	Alcance	1.00	2.00	Bajo
			Tiempo	3.00	6.00	
			Costo	2.00	4.00	
			Calidad	2.00	4.00	
			Total Prob. impacto		16.00	
RG7:	cambio	4.00	Alcance	4.00	16.00	Muy

Cambio de autoridad nominadora durante el proceso de concurso de merito	de la autoridad por solicitud presiden-cial		Tiempo	5.00	20.00	Alto
			Costo	1.00	4.00	
			Calidad	3.00	12.00	
			Total Prob. impacto		52.00	

Datos obtenidos en el campo (Elaboración propia)

3.5.1.3. Riesgos Específico

TABLA 13: Tabla de riesgos específicos

Riesgo	Descripción	Prob.	Obj. afect	Imp	Prob X imp	Tipo RG
RE1	Procesos De meritocra-cias definidos incorrectos	4.00	Alcance	5.00	20.00	Alto
			Tiempo	2.00	8.00	
			Costo	1.00	4.00	
			Calidad	4.00	16.00	
			Total Prob. impacto		48.00	
RE2	Equipo con desconoci-miento del proceso	4.00	Alcance	3.00	12.00	Alto
			Tiempo	3.00	12.00	
			Costo	1.00	4.00	
			Calidad	2.00	8.00	
			Total Prob. impacto		36.00	

RE3	Incorrecta definición de activos de la información en el proceso	3.00	Alcance	2.00	6.00	Alto
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	
			Calidad	4.00	12.00	
			Total impacto	Prob.	36.00	
RE4	Incorrecta definición de los riesgos	3.00	Alcance	2.00	6.00	Alto
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	
			Calidad	4.00	12.00	
			Total impacto	Prob.	36.00	
RE5	incorrectos controles del riesgo	3.00	Alcance	1.00	3.00	Alto
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	
			Calidad	4.00	12.00	
			Total impacto	Prob.	33.00	
RE6	Equipo de Seguridad de la información mal comprometi-	3.00	Alcance	1.00	3.00	Alto
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	
			Calidad	4.00	12.00	
			Total impacto	Prob.	33.00	

	da					
RE7	Desconocimiento de Seguridad de información en el personal TIC	3.00	Alcance	4.00	12.00	Alto
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	
			Calidad	3.00	9.00	
			Total impacto	Prob.	39.00	
RE8	Desconocimiento de los equipos de seguridad de la información sobre el proceso de meritocracia	3.00	Alcance	2.00	6.00	Moderado
			Tiempo	3.00	9.00	
			Costo	1.00	3.00	
			Calidad	3.00	9.00	
			Total impacto	Prob.	27.00	
RE9	Fallas en el cronograma de plan de riesgos	3.00	Alcance	1.00	3.00	Moderado
			Tiempo	5.00	15.00	
			Costo	1.00	3.00	
			Calidad	1.00	3.00	
			Total impacto	Prob.	24.00	
RE10	Demora en	2.00	Alcance	1.00	3.00	Mode-

	la aprobación de política, manuales y procedimien-tos de SI		Tiempo	4.00	12.00	rado
			Costo	1.00	3.00	
			Calidad	1.00	3.00	
			Total Prob. impacto		21.00	
RE11	Incumplimiento de el plan de Seguridad de la información	2.00	Alcance	1.00	3.00	Bajo
			Tiempo	3.00	9.00	
			Costo	1.00	3.00	
			Calidad	1.00	3.00	
			Total Prob. impacto		18.00	

Datos obtenidos en el campo (Elaboración propia)

3.5.2. Respuesta de riesgos del proyecto

3.5.2.1. Riesgos Generales

TABLA 14: Tabla de plan de riesgos generales

RG	Responsable de tratamiento	Plan de mitigación	Plan de contingencia
RG1	Director de proyecto, jefe UTIC y jefe de	- Reunión con los principales de cada área involucrada y	-Personal del apoyo, para actividades pendientes o

	UATH	aprobación del Director de Proyecto.	redundantes. -Liberar actividades no relacionadas con el proyecto.
RG2	Director de proyecto	- Reunión con los principales de cada área involucrada y aprobación del Director de Proyecto.	-La adaptación de los involucrados al proyecto. - Compromiso con el proyecto.
RG3	Director de Proyecto	- Reunión con los principales de cada área involucrada y aprobación del Director de Proyecto.	- Adaptación del cronograma. - Compromiso con el Proyecto.

RG4	Director de Proyecto	- Revisión del Cronograma de Vacaciones. - Ajustes en el cronograma	- Sustitución del personal con perfiles similares
RG5	Responsables de Meritocracia. MRL	-	-
RG6	Jefe de UATH	-	-
RG7	Presidente Del Ecuador	-	-

Datos obtenidos en el campo (Elaboración propia)

3.5.2.2. Riesgos específicos

TABLA 15: Tabla de plan de riesgo específico

RG	Resp. de tratamiento	Plan de mitigación	Plan de contingencia
RE1	Director de Proyecto Jefe de UTIC Jefe de UATH	Cada jefe debe reunirse con su equipo para definir los procesos	Todos los jefes deben solicitar apoyo al director del proyecto
RE2	Jefe UTIC Analista de Seguridad de la Información Analista ISO 27001	Capacitación de manejo de procesos	Subcontratar terceros para elaborar estudio de procesos
RE3	Jefe UTIC Analista de	Implementar las	Realizar reuniones para

	Seguridad de la Información Analista ISO 27001	metodologías	definir los activos
RE4	Jefe UTIC Analista de Seguridad de la Información Analista ISO 27001	Implementar las metodologías	Realizar reuniones para definir riesgos
RE5	Jefe UTIC Analista de Seguridad de la Información Analista ISO 27001	Implementar las metodologías Definir formato para análisis de seguridad a aplicar	Realizar reuniones para análisis de seguridad con normativa

RE6	Jefe UTIC Jefe UATH	Cada jefe hacer Concientizar a su equipo sobre sus funciones	Realizar reuniones y calificar avances de proyecto
RE7	Jefe UTIC Analista de Seguridad de la Información Analista ISO 27001	Capacitar al personal de UTIC	Contratar un tercero
RE8	Jefe UTIC Analista de Seguridad de la Información Analista ISO 27001	Lista de procesos y subproceso donde interfiere riesgos de la informació	Realizar reunión sobre seguridad de la información

		n	
RE9	Director de proyecto		
RE10			
RE11	-	-	-

Datos obtenidos en el campo (Elaboración propia)

3.5.3. Determinación de Salvaguardas

- Reducción del riesgo
- Aceptar el riesgo
- Transferencia del Riesgo
- Evitar el Riesgo

3.5.4. Determinación del riesgo residual

El riesgo residual es aquel riesgo que permanece, luego de haberse implementado controles. Cabe indicar que el grado de riesgo al que está sujeto una organización o compañía no puede eliminarse del todo. Es por eso, que es necesario encontrar un balance entre el nivel de elementos y recursos para disminuir o atemperar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo

residual puede verse como aquello que separa a la compañía de la seguridad absoluta.

El riesgo persiste después de que la dirección desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

Estas acciones pueden incluir:

- Estrategias de diversificación relativas a las concentraciones de clientes
- Las políticas y procedimientos que establezcan límites,
- Autorizaciones y otros protocolos,
- El personal de supervisión para revisar medidas de rendimiento y establecer acciones al respecto
- La automatización de criterios para normalizar y acelerar la toma de decisiones recurrentes y la aprobación de transacciones

Esto puede reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

3.6. Análisis de la Infraestructura de la Gobernación

La infraestructura de la Gobernación del Guayas cuenta con los siguientes equipos:

3.6.1. 3COM 3C17203-US Superstack 3 4400 24port 10/100 Switch

FIGURA 3.23: Switch Superstack 3 4400. Fuente: Datasheet 3com

El SuperStack 3 Switch 4400 de 24 puertos 10/100 combina tecnología de Potencia sobre Ethernet (IEEE-P802.3af) con las características avanzadas, la sencillez, y el estilo de la familia SuperStack 3 Switch 4400. Su diseño de 1-RU compacto y apilable proporciona potencia y datos sobre un mismo cable a cualquier dispositivo compatible, incluyendo teléfonos 3Com NBX, puntos de acceso a LAN inalámbricos, y productos Network Jack.

Potencia sobre Ethernet elimina los costos adicionales de cableado eléctrico y reduce en gran parte el gasto total y el tiempo de instalación, ayudando así a disminuir el costo total de propiedad, especialmente cuando se combina con soluciones de telefonía en red.

El switch soporta todas las características mejoradas del SuperStack 3 Switch 4400, como por ejemplo clasificación y priorización de tráfico, filtrado de tráfico, y log-in de red IEEE 802.1X para seguridad basada en el usuario.

El Switch 4400 PWR puede apilarse junto con otros dispositivos mejorados SuperStack 3 Switch 4400 para formar una pila de switches resistente a fallos de hasta 384 puertos 10/100. Esto permite la distribución de conexiones de alta velocidad a través de la pila (de hasta 4 Gbps), para disponer de conexiones al núcleo de red resistentes frente a fallos y de alta capacidad, incluyendo aquellas que funcionan con tecnología 3Com XRN". Use cualquier módulo SuperStack 3 Switch 4400 para uplinks Gigabit y apilamiento.

La integración en una misma unidad de conectividad de datos y Potencia sobre Ethernet (PoE), permite eliminar las limitaciones de espacio en rack, las preocupaciones de cableado adicional, y la necesidad de múltiples sistemas de respaldo, simplificando así la instalación de dispositivos de networking

Comparte el conjunto de características mejoradas de la familia SuperStack 3 Switch 4400, incluyendo clasificación y priorización avanzada de tráfico de Layer 4, login de red de seguridad mediante RADIUS y control de contabilidad

Solución ideal para instalaciones de telefonía de voz NBX, ya que el switch prioriza automáticamente el tráfico de voz

Alimentación redundante para todas las unidades, usando el 3Com SuperStack Advanced Redundant Power System

Total de Puertos: 24 puertos 10BASE-T/100BASE-TX con auto negociación y Potencia En Línea, conFigurados como MDI/MDIX automático; 2 ranuras para módulos de medios o de apilamiento Interfaces con los Medios: RJ-45

Características:

- Autonegociación full/half-duplex y control de flujo;
- soporte para 802.1Q VLAN, priorización de tráfico 802.1p, DiffServ, Clasificación de Paquetes Multi-Layer;
- Marcaje de Paquetes DiffServ;
- Protocolo de Control de Agregación de Enlaces 802.3ad;
- Login de Red 802.1x mediante RADIUS.
- Power over Ethernet: Estándar en proyecto IEEE P802.3af;
- 15,4W por puerto, 150W en total
- Administración: interfaz de web, administración de interfaz de línea de comandos
- Dimensiones:
    - Altura: 4,4 cm (1,7 in)
    - Anchura: 44 cm (17,3 in)
    - Fondo: 30,4 cm (12,0 in)
    - Peso: 4,6 kg (10,1 lb)

3.6.2. IBM System X3650 M3

Figura 3.24: IBM System X3650 M3. Fuente: Datasheet IBM

El IBM System x3650 M3 ofrece un rendimiento extraordinario para sus aplicaciones más Importantees. Su diseño para un uso eficiente de la energía admite más cores, memoria y capacidad de disco en un paquete 2U ampliable que es fácil de mantener y gestionar. Con más potencia informática por watt y los últimos procesadores Intel ® Xeon®, podrá reducir costos mientras que mantiene la velocidad y la disponibilidad.

El x3650 M3 ofrece un diseño flexible y ampliable y una ruta de actualización sencilla a 16 unidades de disco duro (HDD) o unidades de estado sólido (SSD) y 192 GB de memoria. Sus herramientas de gestión de sistemas, tales como el diagnóstico avanzado, un brazo de gestión de cableado y la capacidad de controlar los recursos desde un único punto, hacen que sea un sistema fácil de implementar, integrar, mantener y gestionar.

TABLA 16: Tabla de resumen de características de IBM System x3650 M3

Formato y altura	Rack/2U
Procesador (máx.)	Hasta dos procesadores Intel Xeon de la serie 5600 a 3.46 GHz de seis cores (3.60 GHz en la versión de cuatro cores) con tecnología QuickPath Interconnect (QPI)
Número de procesadores (est./máx.)	Uno/dos
Memoria caché (máx.)	Hasta 12 MB de nivel 3 (L3)
Memoria (máx.)	Módulos RDIMM (Registered Dual Inline Memory Module) DDR-3 (Double Data Rate 3) de 192 GB a través de 18 ranuras Dual Inline Memory Module (DIMM) o UDIMM (Unregistered DIMM) DDR-3 de 48 GB a través de 12 ranuras DIMM
Ranuras de expansión	Cuatro
Bahías de disco	Hasta dieciséis unidades de disco duro

(total/hot-swap)	(HDD) de 2,5" hot-swap Serial Attached SCSI (SAS)/Serial Advanced Technology Attachment (SATA) o Unidades de estado sólido (SSD) como máximo
Almacenamiento interno máximo	Hasta 16,0 TB (SAS/SATA hot-swap)
Interfaz de red	Dos puertos integrados, además de dos puertos opcionales Gigabit Ethernet (GbE)
Fuente de alimentación (est./máx.)	Una/dos; 460 W CA, 675 W CA, 675 W CA de alta eficiencia o 675 W CC (depende del modelo)
Componentes hot-swap	Fuentes de alimentación, módulos de ventilación, discos
Compatibilidad con RAID	RAID-0, -1, -10 a 6 Gbps o RAID-0, -1, -10, -5, -50 a 6 Gbps con caché de 256 MB o 512 MB y respaldo por batería opcional adicional, según el modelo
Cumplimiento de eficiencia energética	Cumple con las normas de eficiencia energética 80-PLUS y ENERGY STAR (depende del modelo)

Gestión de sistemas	IBM Integrated Management Module (IMM) con Virtual Media Key para la activación de presencia remota opcional, Predictive Failure Analysis, diodos emisores de luz (LED) de diagnóstico, panel Light Path Diagnostics, Automatic Server Restart, IBM Systems Director e IBM Systems Director Active Energy Manager
Sistemas operativos compatibles	Microsoft® Windows® Server2008 R2 y 2008, Red Hat Enterprise Linux® (RHEL), SUSE Linux Enterprise Server (SLES), VMware ESX y ESXi, Oracle Solaris 10 (depende del modelo)

Características sacadas del datasheet de IBM System x3650 M3

3.6.3. IBM DS3512

FIGURA 3.25: IBM DS3512. Fuente: Datasheet IBM

Entre sus características técnicas en cuanto a conectividad se tiene:

- 3 posibles opciones a elegir: SAS, FC/SAS, iSCSI/SAS.
- 4 u 8 puertos host a 6Gbps.
- 8 Gb puertos FC & 4 puertos 6Gbps SAS host.
- 8 puertos iSCSI a 1Gbps & 4 puertos 6Gbps SAS.

En cuanto a escalabilidad, admite hasta 96 unidades de disco:

- SAS de alto rendimiento
- Expansión mediante dos módulos en forma de bandejas.
    - EXP3512 (formato 2U con discos de 3,5″).
    - EXP3524 (formato 2U con discos de 2,5″).
- 2 drive interfaces SAS 6Gbps.
- parte de 1 GB de cache ampliable a 2GB.
- Característica opcional “Rendimiento Turbo”.

Otra de las características adicionales, permite remote mirroring mediante puertos host FC (8 por sistema de almacenamiento). Mayores posibilidades de conectividad y

flexibilidad en conFiguraciones, así como una mayor oferta de puertos.

3.6.4. HP Proliant DL120 G6

FIGURA 3.26: HP Proliant Dl120 G6. Fuente: Datasheet HP

El HP ProLiant DL120 G6 es un servidor para bastidor optimizado, de gama baja y coste reducido. Bajo coste y gran rendimiento. El DL120 G6 admite procesadores Intel. El servidor de 1U y un procesador sencillo son perfectos para infraestructuras informáticas de una sola aplicación, aplicaciones Web o de red. El DL120 G6 proporciona tres ranuras PCI-Express. Pueden llevarse a cabo actualizaciones adicionales, como las de adaptador de bus principal SAS HP y de controladores Smart Array, que proporcionan soporte para unidades de disco duro SAS. La gestión remota que ofrece el LO100i integrado, proporciona al DL120 G6 una solución eficaz

y de bajo coste, para poder administrar los servidores de forma remota en cualquier lugar y en cualquier momento:

- La solución adecuada al precio adecuado
- Fácil de tener y gestionar

Tabla 17: Características generales de HP Proliant DL120 G6

Tipo	Servidor
Uso recomendado	Empresa pequeña, empresa
Factor de forma del producto	Se puede montar en bastidor - 1U
Escalabilidad de servidor	1 vía
Cantidad de compartimentos internos	4
Cantidad de compartimentos frontales	1

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 18: Características procesador / chipset

CPU	Intel Xeon X3430 / 2.4 GHz
Velocidad turbo máx.	2.8 GHz

Número de núcleos	Quad-Core
Computación de 64 bits	Sí
Nº de CPU	1
Nº máximo de CPU	1
Nivel de actualización de CPU	Actualizable
Tipo conjunto de chips	Intel 3420

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 19: Características memoria caché

Tamaño instalado	**8 MB**
Caché por procesador	8 MB

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 20: Características memoria RAM

Tamaño instalado	**4 GB / 16 GB (máx.)**
Tecnología	DDR3 SDRAM - ECC
Velocidad de memoria efectiva	1333 MHz
Velocidad de memoria nominal	1333 MHz
Conforme a la especificación de memoria	PC3-10600
Factor de forma	DIMM de 240 espigas
Características	Sin memoria

	intermedia
Funciones de conFiguración	2 x 2 GB

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 21: Características disco duro

Tipo	HDD
Capacidad	1 x 250 GB
Tipo de interfaz	SATA 3Gb/s
Velocidad del eje	7200 rpm

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 22: Características controlador de almacenamiento

Tipo	1 x SATA
Tipo de controlador interfaz	SATA 3Gb/s
N° canales	6
Nivel RAID	RAID 0, RAID 1

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 23: CARACTERÍSTICAS CONTROLADOR GRÁFICO

Tipo	Integrado
Procesador gráfico	Memoria de vídeo compartida (UMA)

Tamaño de RAM máximo asignado	64 MB
Interfaces de vídeo	VGA

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 24: Características conexión de redes

Tipo	Integrado
Controlador Ethernet	HP NC107i
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 25: Características expansión / conectividad

Bahías	**1 (total) / 0 (libre) x externo Línea delgada de 5,25** **4 (total) / 3 (libre) x interno 3.5" x 1/3H**
Ranuras	1 (total) / 1 (libre) x PCIe x4 - bajo perfil 1 (total) / 1 (libre) x PCIe x16 6 (total) / 4 (libre) x DIMM de 240 patillas 1 (total) / 0 (libre) x CPU
Interfaces	1 x serie 1 x VGA

	4 x USB 1 x LAN (Gigabit Ethernet) 1 x HP iLO

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 26: Característica diverso

Características	Contraseña de administrador, contraseña de encendido, contraseña teclado
Cumplimiento de normas	ACPI 2.0

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 27: Características alimentación

Tipo de dispositivo	Fuente de alimentación
Voltaje nominal	CA 120/230 V (50/60 Hz)
Potencia suministrada	400 vatios

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 28: Características sistemas operativos / software

Servidor Windows	El servidor se prueba, se ajusta y se homologa para Windows Server 2008 R2 con hardware de

certificado	marca de fabricante. Adquiera el kit de opción para distribuidores para obtener la solución precargada.
OS certificado	SUSE Linux Enterprise Server, Microsoft Windows Server, Red Hat Enterprise Linux, SunSoft Solaris x86 10, SunSoft Solaris x64 10

TABLA 29: Características dimensiones y peso

Anchura	44.8 cm
Profundidad	70 cm
Altura	4.3 cm
Peso	14.3 kg

Características sacadas del datasheet de HP Proliant DL120 G6

TABLA 30: Características pará metros de entorno

Temperatura mínima de funcionamiento	10 °C
Temperatura máxima de funcionamiento	35 °C
Ámbito de humedad de funcionamiento	10 - 85%

Características sacadas del datasheet de HP Proliant DL120 G6

- La solución adecuada al precio adecuado. Una matriz de procesadores Intel le permiten elegir el procesador adecuado, de acuerdo con su carga de trabajo. Admite unidades de disco duro SATA y SAS de gran tamaño que proporciona unidades de bajo coste, gran capacidad, alto rendimiento y gran fiabilidad. SATA RAID 0/1 integrado y un array de HBA SAS y controladores Smart Array. Proporciona funciones esenciales para sus necesidades informáticas.

- Fácil de tener y gestionar. Acceso sencillo, chasis de 1U optimizado para bastidor para implantación rápida y mantenimiento eficiente. Ofrece el control para responder con rapidez a problemas del servidor en cualquier lugar que surjan. Acceso a navegador y la interfaz de línea de comandos. Una gestión remota esencial e integrada de gama básica a un precio asequible.

3.6.5. Cisco 1900

Figura 3.27: Cisco 1900. Fuente: Datasheet CISCO

Cisco 1900 Series Integrated Services Routers (ISR) están diseñados para satisfacer las demandas de las aplicaciones de las firmas pequeñas de hoy y evolucionar a los servicios basados en la nube. Ofrecen aplicaciones virtualizadas y colaboración altamente segura a través de la más amplia gama de conectividad WAN de alto rendimiento que ofrece servicios simultáneos de hasta 25 Mbps.

Características y capacidades

Todos los Cisco 1900 Series Integrated Services Routers (ISR) tienen un diseño modular que permite la reutilización de una amplia gama de módulos existentes que satisfagan los requerimientos del negocio y aumentar al máximo la protección de la inversión. Ofrecen:

- **Servicios de aplicaciones ágiles**, incluyendo la capacidad de alojar aplicaciones de terceros Cisco o múltiples en ISM módulos para aplicaciones de misión crítica en la sucursal, junto con los servicios de garantía de entrega de aplicaciones de apoyo a la visibilidad granular de aplicaciones y control de AVC que pueden priorizar y optimizar todos los tipos de datos, voz y aplicaciones de vídeo

- **Conectividad WAN** a través de opciones más amplias de la industria, incluyendo WLAN con 802.11a/g/n, T1/E1, T3/E3, 4G/LTE, xDSL, cobre y fibra Gigabit Ethernet

- **Optimización WAN** con soporte para el router integrado, la optimización WAN en la demanda y la aceleración de aplicaciones a través del módulo de servicio

- **Seguridad altamente integrada** con un conjunto completo de la tecnología VPN con IPSec y SSL VPN mejorados por la aceleración de cifrado integrado, soporte de seguridad para WLAN 802.11i, soporte defensa contra amenazas a través del firewall y sistema de prevención de intrusiones (IPS) Opciones y además incluye soporte para cifrado de última generación y la seguridad basada en la nube.

- **Alto rendimiento** con potentes procesadores y energía eficientes multinúcleo, una tela multigigabit y módulos de servicios de alto rendimiento que se pueden ejecutar múltiples servicios simultáneos ofrecidos de una manera escalable a grandes caudales.

Resumen de Especificaciones:

- Cisco 1900 Series Integrated Services Routers incluyen:

- 2 y 1 unidades RU RU con un máximo de 2 puertos GE integrados WAN

- Hasta 1 Módulo de Servicios Integrados (ISM)

- Hasta 11 puertos de switch LAN, dos ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas

- Acelerada por hardware DES, 3DES y AES de IPSec y SSL VPN

- 802.11a/g/n punto de acceso integrado con 802.11i, WPA y WPA2 para la seguridad

- 16 VLANs inalámbricas y 15 SSIDs

- Optimización WAN a través WAAS exprés

- Acceso a la nube segura con prevención de intrusiones integrado, filtrado de contenidos y seguridad web cloud

3.6.6. Catalyst 3560G

TABLA 31: Características de Catalyst 3560 G

Puertos e Interfaces	
Cantidad de puertos básicos de conmutación RJ-45 Ethernet	8
Peso y dimensiones	
Peso	2,3 kg
Altura	4,4 cm
Ancho	27 cm
Profundidad	23 cm
Control de energía	
Consumo energético	19 W
Certificado Energy Star	
Condiciones ambientales	

Altitud de funcionamiento	0 - 3049 m
Intervalo de humedad relativa para funcionamiento	10 - 85%
Intervalo de temperatura de almacenaje	-25 - 70 °C
Intervalo de temperatura operativa	0 - 45 °C
Altitud no operativa	0 - 4573 m
Protocolos	
Protocolo de trasmisión de datos	Ethernet, Fast Ethernet
Protocolos de gestión	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP
Protocolos de red compatibles	RIP-1, RIP-2, SIPR
Protocolo de conmutación	Ethernet
Red	

Bidireccional completo (Full duplex)	
Estándares de red	IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z
DHCP, cliente	
DHCP, servidor	
Ruteo de IP	
Soporte 10G	
Transmisión de datos	
Tabla de direcciones MAC	12000 entradas
Capacidad de conmutación	32 Gbit/s
Tasa de transferencia (máx)	0,1 Gbit/s
Seguridad	
MAC, filtro de	

direcciones	
Características de administración	
Tipo de interruptor	Gestionado
Otras características	
Dimensiones (Ancho x Profundidad x Altura)	270 x 230 x 44 mm
Software incluido	Cisco IOS IP Base
Tipo de fuente de alimentación	AC
Requisitos de energía	100-240 VAC, 2.5-1.3A, 50-60 Hz
Fuente de alimentación	204 W
Método de autenticación	Kerberos, RADIUS, TACACS+, SSH2
Ranuras de expansión	1x 10/100/1000Base-T/SFP (mini-GBIC)
Tecnología de conectividad	Alámbrico
Características técnicas	ARP, VLAN, IGMP, IPv6
Diseño	

Certificación	CE, FCC Class A certified, UL, TUV GS, cUL, EN 60950, EN55022, NOM, VCCI Class A ITE, IEC 60950, EN55024, UL 60950 Third Edition, CB, AS/NZ 3548 Class A, FCC Part 15, CSA C22.2 No. 60950-00, MIC
Montaje en rack	
Compatibilidad electromagnética	FCC Part 15 Class A, EN 55022 Class A (CISPR22), EN 55024 (CISPR24), AS/NZS CISPR22 Class A, CE, CNS 13438 Class A, MIC, GOST, China EMC
Factor de forma	1U
Indicadores LED	
Color del producto	Azul
Alimentación a través de Ethernet (PoE)	
Energía sobre Ethernet (PoE), soporte	
Desempeño	
Memoria interna	128 MB
Tiempo medio entre	367586 h

fallos	
Memoria Flash	32 MB
Tipo de memoria	RAM
Apilable	

Características sacadas del datasheet de Catalyst 3560 G

CAPÍTULO 4

DISEÑO E IMPLEMENTACION DEL ESQUEMA DE SEGURIDAD

4.1. Alcance del proyecto

Nombre del proyecto: Implementación de un esquema de seguridad de la información del proceso de concurso de méritos y oposición en la Gobernación de la provincia del Guayas basado en el estándar ISO: 27001.

Siglas del proyecto: GG-UTIC-SIA

Justificación del Proyecto: La gobernación de la provincia del Guayas realiza el concurso de méritos y oposición para ganadores del concurso de nombramientos permanentes y conociendo los riesgos de los activos de la información y la afectación que tiene en la reputación de esta institución por la causa de la perdida de la información , Por lo que se realiza el uso de la metodología MARGERIT para la reducción de los riesgos de la información con la aplicación de la normativa ISO 27001, el cual nos ayuda con la revisión de los riesgos y a mitigarlos implantado controles que ayuda a salvaguardar los activos de la información de los procesos de la tecnología, manejo y mejoras continuas alineados a los objetivos.

Descripción del producto: Implementación de un esquema de seguridad de la información del proceso de concurso de méritos y oposición en la Gobernación de la provincia del Guayas basado en el estándar ISO: 27001.

Entregables del Proyecto:

Este proyecto se implementa den la gobernación de la provincia de las guayas:

- Lista de requerimientos
- Soluciones tecnológicas

- Gestión del proyecto
- Planificación de implemento de Seguridad de la Información
- Procesamiento de la información

Procesos a Evaluar:

- Gestión de la documentación.
- Gestión de Recurso Humano.
- Gestión de Meritocracia.
- Gestión de Tecnología de la Información.

Responsables del proyecto:

Jefe de UTIC

Jefe de UTIC

Director de Proyecto

4.2. Organigrama del proyecto

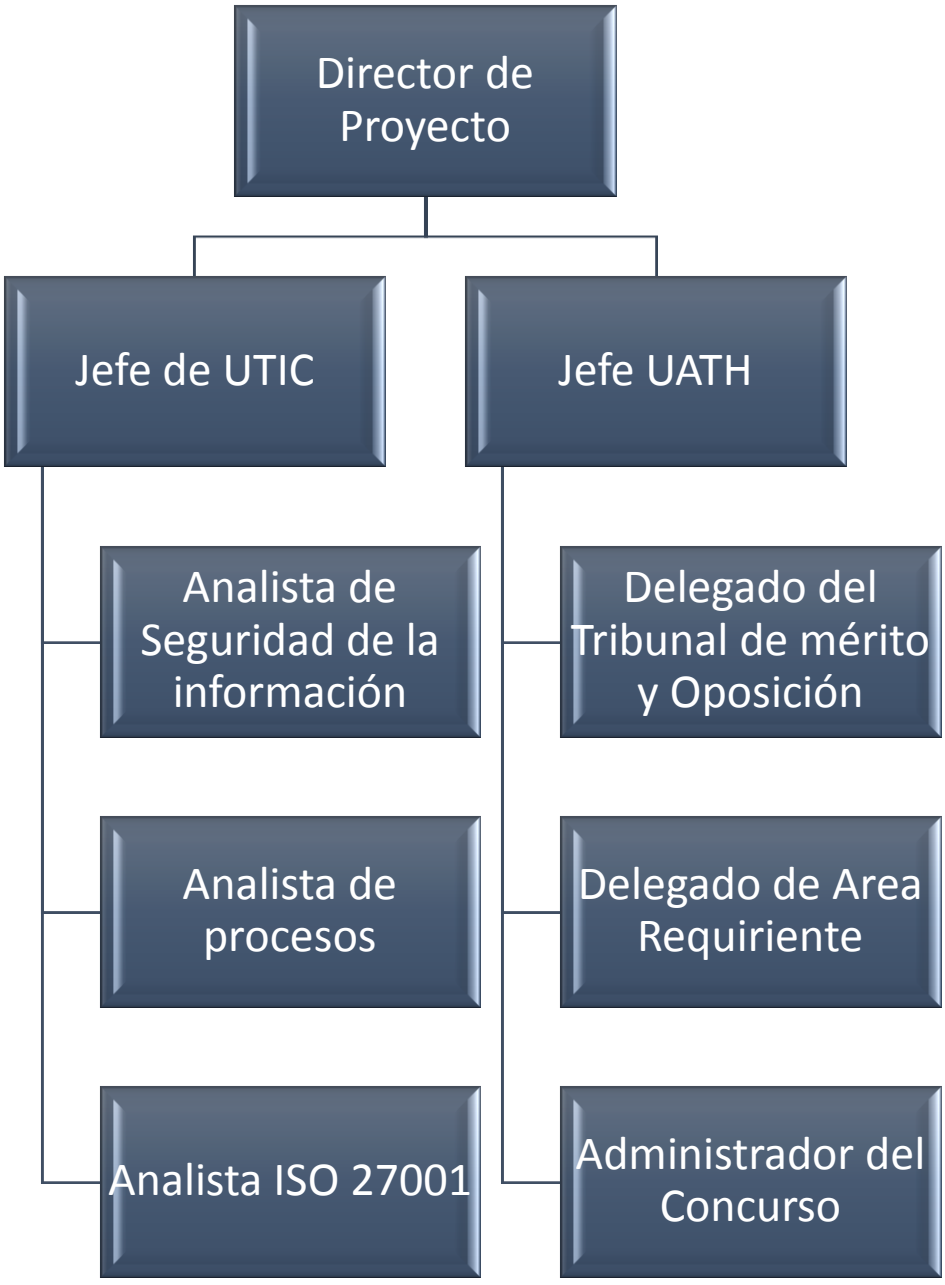


FIGURA 4.28: Organigrama del proyecto. Fuente: Los autores

4.3. Selección de controles basados en la norma ISO 27001

Los controles seleccionados de acuerdo con cada activo de la Gobernación del Guayas son los siguientes:

4.3.1. Activos Gestión Documental

4.3.1.1. Información electrónica

TABLA 32: Cuadro de controles de activos de información electrónica

Amenazas	**Vulnerabilidades**
Manipulación de la información	Métodos o protocolos usados no seguros
A.9 Control de acceso A.9.1 Requisitos del negocio para control de acceso A.9.1.2 Acceso a redes y a servicio en red **Control:** Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	
Mala conFiguración de archivos	Firmas en los documentos electrónicos de seguridad no validados.
A.9 Control de acceso	

<table>
<tr><td colspan="2">A.9.2 Gestión de acceso de usuarios
A.9.2.3 Gestión de derechos de acceso privilegiado
Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.</td></tr>
<tr><td>Robo de correos electrónicos</td><td>Bugs no parchados en el sistema de base de datos</td></tr>
<tr><td colspan="2">A.12 Seguridad de las operaciones
A.12.6 Gestión de la vulnerabilidad técnica
A.12.6.1 Gestión de las vulnerabilidades técnicas
Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.</td></tr>
<tr><td>Robo de información en equipos</td><td>Contraseñas débiles en correos y equipos computacionales.</td></tr>
<tr><td colspan="2">A.9 Control de acceso
A.9.4 Restricción de acceso a la información
A.9.4.3 Sistema de gestión de contraseñas
Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las</td></tr>
</table>

contraseñas

Datos obtenidos en el campo (Elaboración propia)

4.3.1.2. Información escrita

TABLA 33: Cuadro de controles de activos de información escrita

Amenazas	**Vulnerabilidades**
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.1 Áreas seguras A.11.1.1 Perímetro de seguridad física **Control:** Se deben definir y usar perímetros de seguridad y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	
Daño por agua	Desastres naturales
A.11 Seguridad física y del entorno A.11.1 Áreas seguras A.11.1.4 Protección contra amenazas externas y ambientales	

Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes	
Desastres naturales	Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.1 Áreas seguras A.11.1.4 Protección contra amenazas externas y ambientales **Control:** Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes	

Datos obtenidos en el campo (Elaboración propia)

4.3.1.3. Información hablada

TABLA 34: Cuadro de controles de activos de información hablada

Amenazas	Vulnerabilidades
Manipulación de la	No actualización en los firmwares de equipos de videoconferencia,

información	teléfonos
A.13 Seguridad de las comunicaciones A.13.1 Gestión de la seguridad de las redes A.13.1.1 Controles de redes **Control**: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	

Datos obtenidos en el campo (Elaboración propia)

4.3.2. Activo de Software

4.3.2.1. Sistema operativo

TABLA 35: Cuadro de controles de activos de sistema operativo

Amenazas	Vulnerabilidades
Mala conFiguración de archivos del sistema	No aplicaciones de actualizaciones críticas al sistema operativo
A.12.5 Control de software operacional A.12.5.1 Instalación de software en sistemas operativos **Control:** Se deben implementar procedimientos para	

controlar la instalación de software en sistemas operativos

Datos obtenidos en el campo (Elaboración propia)

4.3.2.2. Software de herramientas utilitarias

TABLA 36: Cuadro de controles de activos de software de herramientas utilitarias

Amenazas	Vulnerabilidades
Instalación de utilitarios de manera ilegal	Ejecución de código malicioso al no ser de fuente confiable
A.12.2 Protección contra códigos maliciosos A.12.2.1 Controles contra códigos maliciosos **Control:** Se deben implementar controles de detección, de prevención, y de recuperación, combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos.	

A.9.4 Control de acceso a sistemas y aplicaciones A.9.4.4 Uso de programas utilitarios privilegiados **Control:** Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Datos obtenidos en el campo (Elaboración propia)

4.3.2.3. Software de protección

TABLA 37: Cuadro de controles de activos de software de protección

Amenazas	Vulnerabilidades
Instalación de software de protección de manera ilegal	Abertura de backdoors sin conocimiento del administrador
A.12.5 Control de software operacional A.12.5.1 Instalación de software en sistemas	

operativos **Control:** Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos A.12.6 Gestión de la vulnerabilidad técnica A.12.6.2 Restricción sobre la instalación de software **Control**: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios

Datos obtenidos en el campo (Elaboración propia)

4.3.2.4. Software de administración de la base de datos

TABLA 38: Cuadro de controles de activos de software de administración de base de datos

Amenazas	Vulnerabilidades
Mala conFiguración de los archivos de conFiguración de la base de datos	No tener actualizado la base de datos con las últimas correcciones

mySQL	
A.9 Control de acceso A.9.4 Control de acceso a sistemas y aplicaciones A.9.4.5 Control de acceso a códigos fuente de programas **Control:** Se debe restringir el acceso a los códigos fuente de los programas	

Datos obtenidos en el campo (Elaboración propia)

4.3.3. Activos Fijos

El objetivo es prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.

4.3.3.1. Hardware de procesamiento

TABLA 39: Cuadro de controles de activos de hardware de procesamiento

Amenazas	Vulnerabilidades
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.2 Equipos	

A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado	
Desastres naturales	Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control**: Los equipos deben estar ubicados y	

protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado

Datos obtenidos en el campo (Elaboración propia)

4.3.3.2. Hardware de comunicación

TABLA 40: Cuadro de controles de activos de hardware de comunicación

Amenazas	**Vulnerabilidades**
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.3 Seguridad del cableado **Control**: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno	

A.11.2 Equipos A.11.2.2 Servicio de suministro **Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
Desastres naturales	Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado.	

Datos obtenidos en el campo (Elaboración propia)

4.3.3.3. Hardware de almacenamiento

TABLA 41: Cuadro de controles de activos de hardware de almacenamiento

Amenazas	Vulnerabilidades
Fuego	Falta de protección contra fuego

A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.3 Seguridad del cableado **Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.2 Servicio de suministro **Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
Desastres naturales	Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y	

peligros del entorno y las posibilidades de acceso no autorizado.

Datos obtenidos en el campo (Elaboración propia)

4.3.3.4. Mobiliario y equipamiento

TABLA 42: CUADRO DE CONTROLES DE ACTIVOS DE MOBILIARIO y equipamiento

Amenazas	Vulnerabilidades
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.3 Seguridad del cableado **Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.2 Servicio de suministro	

Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
Desastres naturales | Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado.

Datos obtenidos en el campo (Elaboración propia)

4.3.3.5. Equipos de oficina

TABLA 43: Cuadro de controles de activos de equipos de oficina

Amenazas	Vulnerabilidades
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.2 Equipos	

A.11.2.3 Seguridad del cableado **Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.2 Servicio de suministro **Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
Desastres naturales	Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones **Control**: **FALTA**	

Cortes de electricidad	Falta de UPS en el edificio de la Gobernación
A.11 Seguridad A.11.2 Equipos A.11.2.2 Servicios de suministro **Control**: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	

Datos obtenidos en el campo (Elaboración propia)

4.3.4. Activos de Servicios

4.3.4.1. Comunicación

TABLA 44: Cuadro de controles de activos de comunicación

Amenazas	Vulnerabilidades
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.3 Seguridad del cableado **Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a	

los servicios de información se debe proteger contra interceptación, interferencia o daño	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.2 Servicio de suministro **Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
Desastres naturales	Condición local no adecuada para desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado.	

Datos obtenidos en el campo (Elaboración propia)

4.3.4.2. Servicio general

TABLA 45: Cuadro de controles de activos de servicio general

Amenazas	Vulnerabilidades
Fuego	Falta de protección contra fuego
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.3 Seguridad del cableado **Control:** El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño	
Daño por agua	Falta de protección física
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.2 Servicio de suministro **Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	
Desastres	Condición local no adecuada para

naturales	desastres
A.11 Seguridad física y del entorno A.11.2 Equipos A.11.2.1 Ubicación y protección de los equipos **Control:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado.	

Datos obtenidos en el campo (Elaboración propia)

4.3.4.3. Servicios de Concurso de méritos y oposición

TABLA 46: Cuadro de controles de activos de servicios de concurso de méritos y oposición

Amenazas	Vulnerabilidades
Fuga de información	La falta de normativas sobre el uso y políticas de la información
A.5 Políticas de la seguridad de la información A.5.1 Orientación de la dirección para la gestión de la seguridad de la información A.5.1.1 Políticas para la seguridad de la información **Control:** Se debe definir un conjunto de políticas	

para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados, y a las partes externas pertinentes	
Incumplimiento de legislación	Falta de conocimiento en las leyes y normas de concurso por parte de los administradores
A.5. Políticas de la seguridad de la información A.5.1.2 Revisión de las políticas para la seguridad de la información **Control:** Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	
Uso mal intencionado de los recursos	Insuficiencia en la seguridad de la información
A.8 Gestión de activos A.8.1 Responsabilidad por los activos A.8.1.3 Uso aceptable de los activos **Control:** Se deben identificar, documentar e	

implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procedimientos de información. A.8.2 Clasificación de la información A.8.2.3 Manejo de activos **Control**: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización

Datos obtenidos en el campo (Elaboración propia)

4.3.5. Activos de funcionarios

4.3.5.1. Jefa de Recursos Humanos (Responsable de la UATH)

TABLA 47: Cuadro de controles de activos de la jefa de recursos humanos (responsable de la UATH)

Amenazas	Vulnerabilidades
Incumplimiento de la legislación	Falta de conocimiento de los acuerdos ministeriales
A.7 Seguridad de los recursos humanos	

A.7.1 Antes de asumir el empleo A.7.1.1 **Control:** Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.

Datos obtenidos en el campo (Elaboración propia)

4.3.5.2. Delegado al tribunal de Méritos y oposición

TABLA 48: Cuadro de controles de activos del delegado al tribunal de méritos y oposición

Amenazas	Vulnerabilidades
Incumplimiento de la legislación	Falta de conocimiento de los acuerdos ministeriales
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo	

A.7.2.1 Responsabilidades de la dirección **Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	
Divulgación de la información	Falta de normativas del manejo de la información
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.3 Proceso disciplinario **Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	

Datos obtenidos en el campo (Elaboración propia)

4.3.5.3. Responsable de la unidad Administrativa de la vacante del puesto

TABLA 49: Cuadro de controles de activos de responsable de la unidad administrativa de la vacante del puesto

Amenazas	Vulnerabilidades
Incumplimiento de la legislación	Falta de conocimiento de los acuerdos ministeriales
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.1 Responsabilidades de la dirección **Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	
Divulgación de la información	Falta de normativas del manejo de la información
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.3 Proceso disciplinario **Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	

Datos obtenidos en el campo (Elaboración propia)

4.3.5.4. Analista 1 de Recursos Humanos (Administrador de SocioEmpleo)

TABLA 50: Cuadro de controles de activos de analista 1 de recursos humano (administrador de SocioEmpleo)

Amenazas	Vulnerabilidades
Incumplimiento de la legislación	Falta de conocimiento de los acuerdos ministeriales
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.1 Responsabilidades de la dirección **Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	
Divulgación de la información	Falta de normativas del manejo de la información
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.3 Proceso disciplinario	

Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Datos obtenidos en el campo (Elaboración propia)

4.3.5.5. Analista 2 de Recursos Humanos (Administrador del Concurso)

TABLA 51: Cuadro de controles de activos de analista 2 de recursos humano (administrador del concurso)

Amenazas	Vulnerabilidades
Incumplimiento de la legislación	Falta de conocimiento de los acuerdos ministeriales
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.1 Responsabilidades de la dirección **Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las	

políticas y procedimientos establecidos por la organización.	
Divulgación de la información	Falta de normativas del manejo de la información
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.3 Proceso disciplinario **Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	

Datos obtenidos en el campo (Elaboración propia)

4.3.5.6. Servidor público de apoyo 4 (Responsable de Secretaría)

TABLA 52: Cuadro de controles de activos de servidor público de apoyo 4 (responsable de secretaría)

Amenazas	Vulnerabilidades
Incumplimiento de la	Falta de conocimiento de los acuerdos ministeriales

legislación	
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.1 Responsabilidades de la dirección **Control:** La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	
Divulgación de la información	Falta de normativas del manejo de la información
A.7 Seguridad de los recursos humanos A.7.2 Durante la ejecución del empleo A.7.2.3 Proceso disciplinario **Control:** Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	

Datos obtenidos en el campo (Elaboración propia)

4.4. Definición de la política de seguridad para el proceso

El principal objetivo de la definición de la política de seguridad para el proceso mérito y oposición es que la alta dirección defina lo que quiere conseguir al implementar la norma ISO 270001 en cuanto a la seguridad de la información en la Gobernación del Guayas.

Otro objetivo es la creación de un documento en el cual los directores y jefes de las áreas involucradas comprendan de forma fácil las metas, que les ayudarán a controlar lo que suceda dentro del Sistema de Gestión de Seguridad de la Información.

La norma ISO 27001 dice lo siguiente respecto a la política de seguridad:

- La política tiene que adaptarse a la empresa, es decir, que no se puede copiar la política de una empresa y usarla en otra organización.
- Se debe definir un marco para establecer todos los objetivos de seguridad de la información,
- Tiene que mostrar el compromiso de la alta dirección para así cumplir con los requerimientos de las partes interesadas mejorando el Sistema de Gestión de Seguridad de la Información.

- Debe ser comunicada dentro de la organización y a todas las partes interesadas, definiendo el responsable de tal comunicación y de manera continua.
- Revisada continuamente por el propietario de la política definida. Esta persona será responsable de conservar la política.

De ser la organización a la cual se aplica una política de seguridad pequeña, se puede incluir los siguientes apartados:

- Alcance del Sistema de Gestión de Seguridad de la Información.
- Responsabilidades de las partes fundamentales del Sistema de Gestión de la Seguridad de la Información: responsable de las operaciones, coordinación, a nivel ejecutivo, evaluación de riesgos, incidentes, auditorías internas, etc.
- Medición: objetivos de seguridad de la información alcanzados, Resultados reportados, etc.

4.4.1. Objetivo

La dirección de Gobernación del Guayas, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de

seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos y las ciudadanas de la provincia del Guayas, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

4.4.2. Alcance

Esta política es aplicable a todos los colaboradores, proveedores, terceras partes que usen activos de información que sean propiedad de la Gobernación del Guayas.

4.4.3. Descripción de las políticas y estándares

4.4.3.1. Generalidades

Para Gobernación del Guayas, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

4.4.4. Organización de seguridad

4.4.4.1. Política de la organización de seguridad

Esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más Importantees de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de la ciudadanía, proveedores y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, practicantes y ciudadanía de la Gobernación del Guayas
- Garantizar la continuidad del negocio frente a incidentes.
- Gobernación del Guayas ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Estándares de la política de la organización de seguridad

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de Gobernación del Guayas:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, o terceros.

- GOBERNACIÓN DEL GUAYAS protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o ciudadanía)

- GOBERNACIÓN DEL GUAYAS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- GOBERNACIÓN DEL GUAYAS protegerá su información de las amenazas originadas por parte del personal.

- GOBERNACIÓN DEL GUAYAS protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- GOBERNACIÓN DEL GUAYAS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- GOBERNACIÓN DEL GUAYAS implementará control de acceso a la información, sistemas y recursos de red.

- GOBERNACIÓN DEL GUAYAS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- GOBERNACIÓN DEL GUAYAS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- GOBERNACIÓN DEL GUAYAS garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- GOBERNACIÓN DEL GUAYAS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

4.4.5. Uso aceptable de los activos y recursos

4.4.5.1. Política de uso aceptable de los activos y recursos de información

Todos los trabajadores, colaboradores, contratistas, terceras partes, que usen activos de información que pertenezcan a la Gobernación del Guayas, son

responsables de cumplir y acoger con integridad la Política de uso aceptable de los activos y recursos de información para dar un uso legítimo y eficiente a los recursos asignados.

4.4.5.2. Estándares para el uso aceptable de los activos de información

Uso de los sistemas y equipos de cómputo

La Gobernación del Guayas tiene una leyenda al inicio de sesión en los equipos de cómputo:

“Advertencia! Este sistema, así como la información en él contenida es propiedad de la Gobernación del Guayas y su uso está restringido únicamente para propósitos en beneficio de la ciudadanía guayaquileña, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y

utilización de este sistema implica su consentimiento con esta política.

Correo electrónico

Las comunicaciones por email entre los funcionarios de la Gobernación del Guayas, trabajadores, contratistas, proveedores y/o terceras partes deben hacerse a través del correo proporcionado por la Gobernación del Guayas. No se permite utilizar cuentas personales para comunicarse con los mismos trabajadores ni para transmitir cualquier otro tipo de información de la Gobernación.

A los trabajadores que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados. La jefa de la Unidad Administrativa de Talento Humano (UATH) es la responsable de informar a la jefa de la Unidad de Tecnología de la Información y Comunicación (UTIC) a través del Quipux, las vinculaciones que requieran

creación de cuentas de correo; de igual manera debe informar oportunamente los retiros de los trabajadores para la suspensión de este servicio.

La cuenta de correo se mantendrá activa mientras el trabajador labore en la Gobernación, exceptuando casos de fuerza mayor o mal uso que puedan luego causar la suspensión o cancelación de la misma. Una vez el que el trabajador se desvincula, la cuenta es dada de baja en el servidor mediante un memo enviado por la jefa de la UATH a través del Quipux a la jefa de la UTIC.

La capacidad de almacenamiento máxima de correo electrónico para todos los trabajadores es de 1GB independiente del tipo de usuario. Sin embargo, en caso de necesidades especiales, el interesado podrá solicitar el aumento de la capacidad. De la misma manera, en caso de necesidad (negocio o técnicas), las capacidades máximas de los buzones de correo electrónico

podrán ser modificadas por parte de la jefa de UTIC.

El sistema de filtrado y monitoreo del servicio de correo electrónico de la Gobernación del Guayas revisará los archivos adjuntos a los mensajes de correo electrónico recibido por los trabajadores, para verificar la presencia de virus o malware.

Gobernación del Guayas tiene regla de renuncia que se deben utilizar siempre en los mensajes. Para evitar reclamaciones legales tienen que hacer pública la renuncia de responsabilidad legal por el envío de la información. El texto aprobado es:

“La información contenida en este mensaje y en sus anexos es estrictamente confidencial. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío a la dirección electrónica del remitente y bórrela puesto que su uso no

autorizado acarreará las sanciones y medidas legales a que haya lugar. La institución no se hace responsable por la presencia en este mensaje o en sus anexos, de algún virus o malware que pueda generar o genere daños en sus equipos, programas o afecte su información."

El buzón de correo electrónico es personal e intransferible y concierne al trabajador guardar seguridad protegiendo su clave de acceso. El usuario del correo electrónico es la única persona responsable por el buen uso de su cuenta. Es por eso, que al aceptar el buzón entregado por la jefe de las UTIC, el usuario se compromete a:

- Respetar la privacidad de las cuentas de otros usuarios de la Gobernación del Guayas.
- Usar el correo electrónico para enviar y recibir mensajes pertinentes para el desarrollo de las labores propias de su cargo.
- Actuar con cortesía y respeto.

- No crear, distribuir o reenviar mensajes que ofendan la intimidad, dignidad de las personas, de las instituciones o realizar algún tipo de acoso, calumnia, difamación, con intención de insultar o cualquier otra forma de actividad hostil.
- No usar la cuenta para el envío o reenvío de mensajes spam (no deseados, no solicitados o de remitente desconocido), hoax (intento de hacer creer que algo falso es real), con contenido que pueda ser ofensivo o dañino para otros usuarios (virus o pornografía), o que sea contrario a las políticas y normas institucionales.
- Realizar mantenimiento periódico del correo, cuando el sistema le haga advertencias de espacio disponible.
- Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas desconocidas.

Navegación en internet

El uso de internet debe estar reservado exclusivamente para el cumplimiento de las actividades de la Gobernación del Guayas y deben ser utilizados para las funciones establecidas a su cargo, por lo que se deben tomar en cuenta los siguientes parámetros:

- El usuario tiene prohibido descargar programas que realicen conexiones automáticas o ingreso a URL clasificados con contenido pornográfico y el uso de los recursos computacionales para la distribución o reproducción de este tipo de material, ya sea a través de medios web o magnéticos (unidades de CD, pen drives, discos extraíbles)

- Evitar el uso de servicios de descarga como: utorrent, bittorrent, emule o similares

- La descarga de música y videos no es una práctica permitida.

Uso de herramientas que comprometen la seguridad

Hacer o intentar hacer, sin permiso del jefe de la UTIC, cualquiera de los siguientes actos:

- Monitorear datos o tráfico
- Acceder a servidores, sistema o red
- Probar firewalls o herramientas de hacking
- Atentar contra la vulnerabilidad del sistema o redes
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

Recursos compartidos

El uso de carpetas compartidas en los equipos de cómputo de los usuarios, aunque puede ser útil como herramienta laboral, posee algunos riesgos que afectan los principios de confidencialidad, integridad y disponibilidad de la información, por lo que su uso debe ser

autorizado y controlado. Los siguientes lineamientos se definen para su uso seguro y óptimo:

- la UTIC estable e implementa, en caso de ser aprobado, la conFiguración de acceso a la carpeta compartida, previo requerimiento formal a través del Quipux.
- Definir el tipo de acceso y los roles necesarios sobre la carpeta (lectura, escritura, modificación y/o borrado)
- Utilizar las carpetas destinadas en el servidor de archivos cuando de información confidencial se tratase, e incluirlas en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.
- El acceso a carpetas compartidas debe restringirse a los usuarios que los necesiten y deben ser protegidas con contraseñas.

- Los accesos a las carpetas compartidas no son permitidas a equipos de usuarios que no cuenten con antivirus corporativo actualizado.

4.5. Tratamiento y gestión del riesgo en seguridad de la información

Este seguimiento de la documentación será controlado y evaluado por la secretaría general.

El incumplimiento a la política de Seguridad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Gobernación del Guayas, incluyendo lo establecido en las normas que competen al Gobierno Nacional del Ecuador en cuanto a Seguridad y Privacidad de la Información se refiere.

4.6. Difusión de política y los procedimientos

Las políticas de acceso a la información serán difundidas mediante correo el electrónico, memorando u oficios utilizando la plataforma de Quipux, con documentos electrónicos que tengan firma digital.

Esta documentación debe ser monitoreada y ver el recorrido del documento hasta que llegue a el estado de archivado, cada proceso que transcurra en la documentación debe ser con fecha tope de respuesta

establecida en cada uno de los procesos de los concursos de mérito y oposición de la Gobernación de la provincia del Guayas.

CAPÍTULO 5

DESARROLLO Y RESULTADOS DE LAS PRUEBAS DEL ESQUEMA DE SEGURIDAD

5.1. Definición de escenario de pruebas

Se tomaron en cuenta los activos (computadoras de escritorio, laptops, impresoras, equipos de comunicación) de los departamentos de Recursos Humanos y Tecnología de la Gobernación del Guayas.

Para realizar las pruebas de escaneo de vulnerabilidades se usaron dos herramientas. La primera es MBSA (Microsoft Baseline Security Analyzer) y la segunda es Insight Rapid7.

5.1.1. Microsoft Baseline Security Analyzer

El analizar de seguridad de base de Microsoft (MSBA, por sus siglas en inglés) provee un método sencillo para identificar actualizaciones de seguridad no instaladas, packs de servicio en los equipos y mal conFiguraciones se seguridad comunes. La versión 2.3 añade soporte para equipos con sistemas operativos Windows 8.1, Windows 8, Windows Server 2012 R2 y Windows Server 2012 adicionalmente brinda soporte con las versiones anteriores como Windows Server 2008 R2, Windows 7, Windows Vista, Windows Server 2003 y Windows XP. Windows 2000 ya no es soportado con la nueva versión.

MSBA no escanea ni reporta actualizaciones de no seguridad no instalados, herramientas o drivers de terceros.

5.1.1.1. Instalación de MBSA

Previo a esto se tiene que asegurar que la versión descarga es la última. Esto puede ser visto al hacer clic derecho en el instalador. Seleccionamos propiedades y se dirige a la pestaña Detalles. Ahí se ve el Build: 2211 que es la última versión como se muestra en la Figura 1.

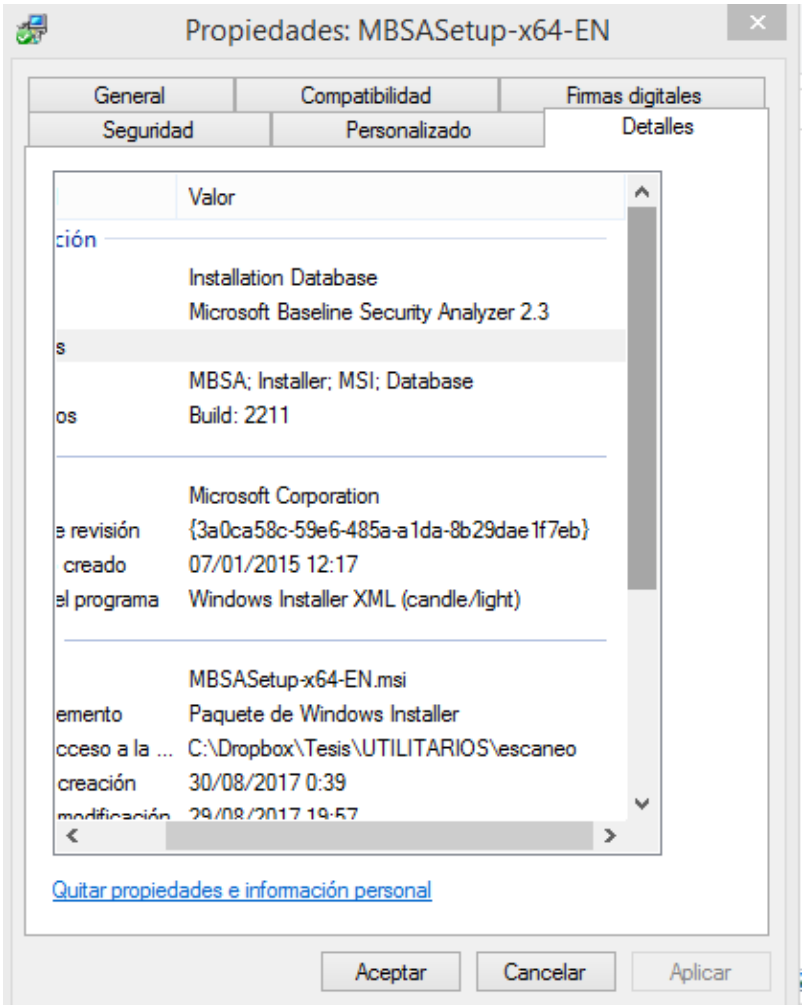


FIGURA 5.29: Propiedades mbsaseptup-x64. Fuente: Los autores

Luego se procede a instalar el programa. Aparece una pantalla como la que se muestra a continuación.

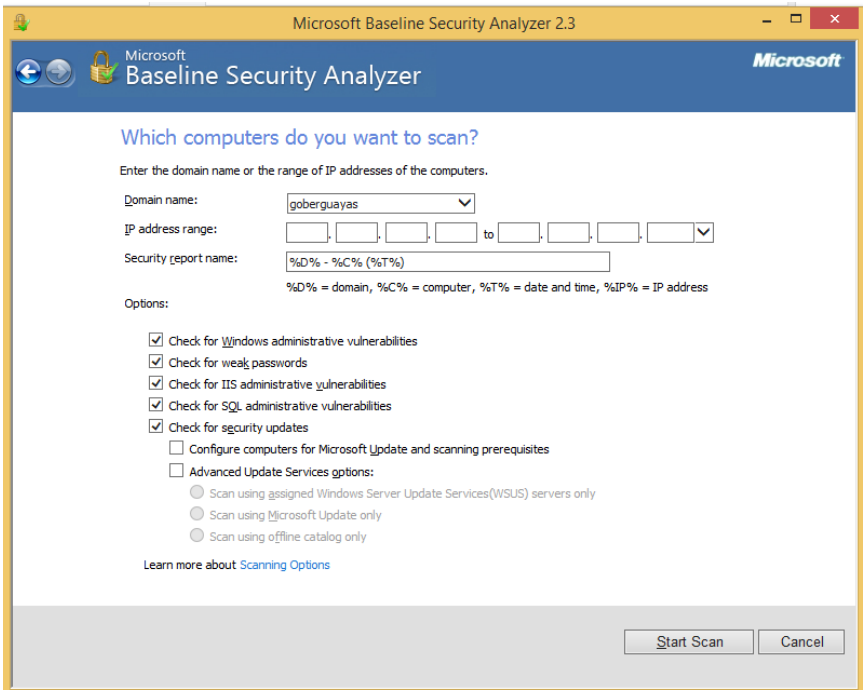


FIGURA 5.30: Ventana de instalación de Microsoft Baseline Security Analyzer. Fuente: Los autores

La información que se tiene que llenar es la siguiente:

- Si los equipos computacionales no forman parte de un controlador de dominio, se escriben los rangos de las direcciones ip en el apartado **IP address range.**

- Si los equipos computacionales forman parte de un controlador de dominio, se escribe el nombre del

dominio al cual pertenecen, en este caso el dominio es GOBERGUAYAS:

- Se deben seleccionar las siguientes opciones:
    - Chequear vulnerabilidades administrativas de Windows.
    - Chequear contraseñas débiles.
    - Chequear vulnerabilidades administrativas de IIS.
    - Chequear vulnerabilidades administrativas de SQL.
    - Chequear actualizaciones de seguridad.

Terminado esto, se da clic en **Start Scan** el cual descargará información de actualizaciones de seguridad desde los servidores de Microsoft, por lo que es necesario que el equipo cuente con conexión a internet. Al ser la primera vez que se ejecuta el programa, la descarga de la información demorará. Luego de esto, empieza a escanear las vulnerabilidades del equipo o equipos indicados en los apartados anteriores y al finalizar genera el reporte respectivo.

5.1.2. InsightVM

La Seguridad Adaptativa y el Monitoreo en Vivo de InsightVM da al programa de administración de vulnerabilidades información al día, puntajes de riesgo granular, y el conocimiento de lo pueden estar buscando los atacantes. Con esto es posible actuar de manera inmediata.

Entre las características que cuenta la herramienta InsightVM se tienen:

- Monitoreo en tiempo real de las vulnerabilidades: Recolecta información reciente y de manera automática evalúa los cambios y las brechas, reduciendo la remediación en cuestión de minutos con una vista en video en las vulnerabilidades mientras suceden.

- Bloquea los puntos finales cambiantes de los usuarios: Se beneficia del monitoreo en vivo de los endpints, ya sea usando la Seguridad Adaptativa o los agentes Rapid7, para llevar el control de los trabajadores remotos y los nuevos dispositivos.

- Implementa conFiguraciones seguras: brinda el sistema basado en las mejores prácticas de la industria tales como CIS (Center for Internet Security) y DISA (Defense Information Systems Agency) STIG (Security Technical Implementation Guide) para que la red esté asegurada.

- Adapta a los ambientes cambiantes: usando la Seguridad Adaptativa de InsightVM, automáticamente detecta y escanea los nuevos dispositivos apenas entran a la red e identifica cuáles tienen vulnerabilidades criticas tan pronto sean liberadas.

- Escalabilidad es la clave: Ya sea que sea una empresa pequeña o escáner un millón de IPs cada día, las capacidades de descubrimiento avanzado y la analítica de la nube de InsightVM (incluyendo la integración con VMWare y DHCP) hacen fácil administrar los programas de administración de vulnerabilidad de cualquier tamaño.

5.1.2.1. Configuración de la herramienta InsightVM

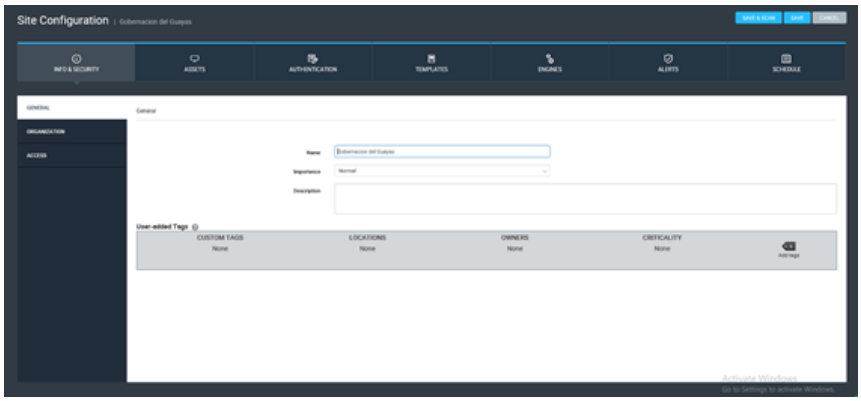


FIGURA 5.31: ConFiguración de sitio – general. Fuente: Los autores

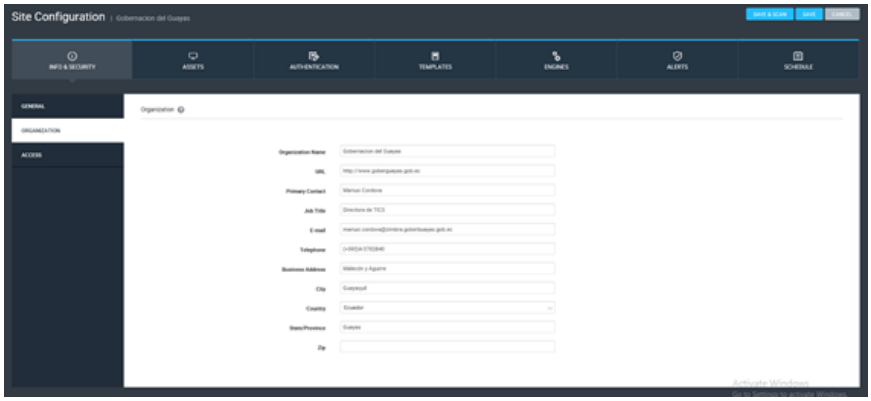


FIGURA 5.32: ConFiguración de sitio – organización. Fuente: Los autores

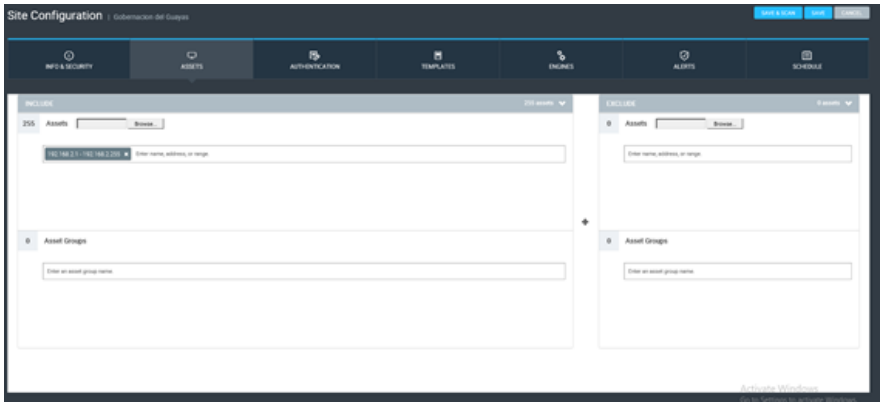


FIGURA 5.33: ConFiguración de sitio – activos. Fuente: Los autores

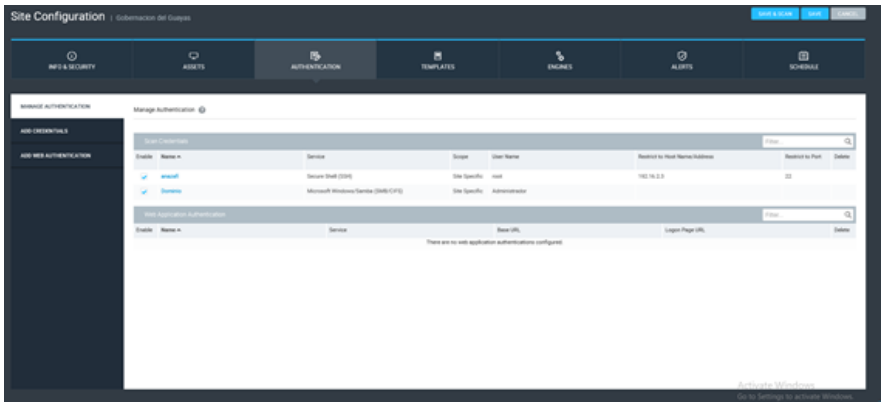


FIGURA 5.34: ConFiguración de sitio – autenticación-administrar autenticación. Fuente: Los autores

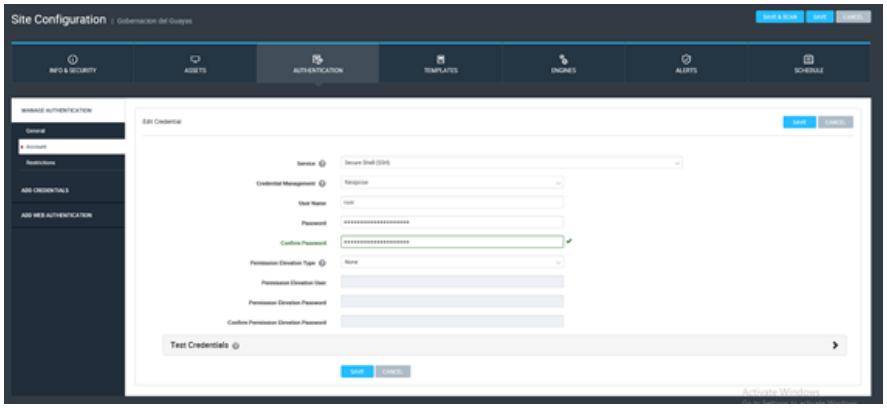


FIGURA 5.35: ConFiguración de sitio – autenticación- administrar autenticación. Fuente: Los autores

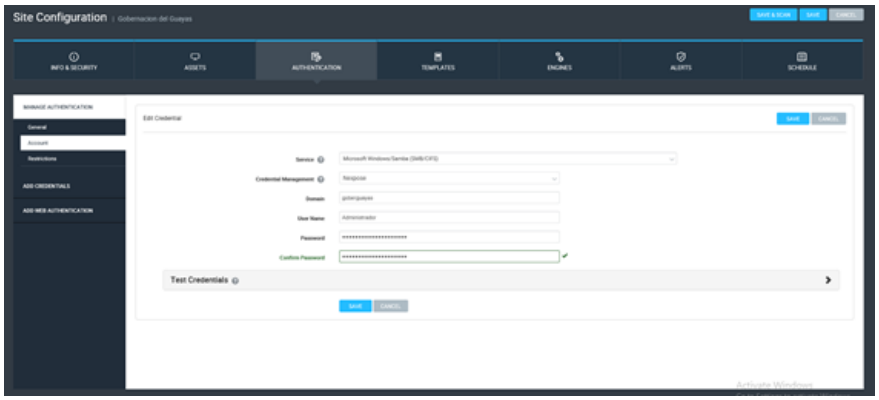


FIGURA 5.36: ConFiguración De Sitio – Autenticación – Administrar Autenticación – Cuenta. Fuente: Los Autores

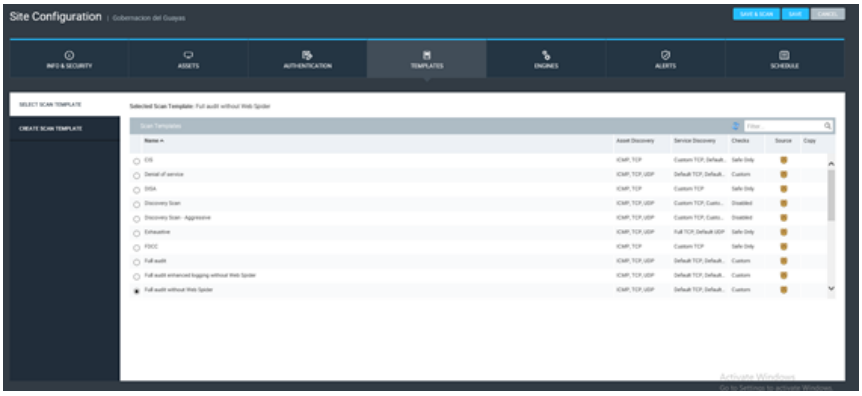


FIGURA 5.37: ConFiguración De Sitio – Plantillas. Fuente: Los Autores

5.2. Pruebas sobre los riesgos en los activos principales del proceso

TABLA 53: Activos computacionales de la Gobernación del Guayas

IP	Nombre	SO	Exp	Malware	Vuln.	Riesgo
192.168.2.1		D-Link embedded	1	0	15	53744756
192.168.2.3		Linux 2.6.18-238.12.1.el5	11	0	14	4285223
192.168.2.4	Servidor	Microsoft Windo	6	0	62	16244292

		ws Server 2008 R2 SP1				
192.168.2.5			0	0	0	0
192.168.2.6	NO-TE-AGUANTO	Apple Mac OS X 10.10	56	0	661	25296834
192.168.2.12		Linux 2.6.9	0	0	3	50556198
192.168.2.13		3Com embedded	0	0	2	50556198
192.168.2.16			0	0	1	0
192.168.2.17		Dish embedded	0	0	4	0
192.168.2.19		AXIS embedded	0	0	3	0
192.168.2.20		Microsoft Windows 7	0	0	4	0

192.168.2.21	GYSTIC001	Microsoft Windows 7 Professional Edition	7	1	8	31301448
192.168.2.24	TIC005	Microsoft Windows 10	0	0	7	30598958
192.168.2.29			0	0	0	0
192.168.2.40	HP_DESPACHO	HP 700 color MFP M775	2	0	35	15696301
192.168.2.44	COM005	Microsoft Windows 7.5	0	0	0	0
192.168.2.50	ET0021B7F0108B	Lexmark X656de	3	0	24	11002695
192.168.2.56	DIGITA	Micros	14	1	18	7911926

	L	oft Windows 7 Professional Edition				
192.168.2.63	UA001	Microsoft Windows 7 Professional Edition	7	1	7	39786458
192.168.2.78	USER-PC	Microsoft Windows 7 Home	7	1	4	25470186
192.168.2.79			0	0	0	0
192.168.2.83	GYSSEC0003	Microsoft Windows 7 Professional Edition	7	1	6	25470186

192.168.2.92	GYSULJ0002	Microsoft Windows Server 2008	0	0	3	0
192.168.2.102	COM006	Microsoft Windows 7.5	0	0	0	0
192.168.2.116			0	0	1	0
192.168.2.120	RRHH	Xerox WorkCentre 4260	0	0	5	25712378
192.168.2.130	GOBERNACION_UPI	Xerox WorkCentre 4260	0	0	5	25712378
192.168.2.139	GYSUAF0010-PC	Microsoft Windows 7 Professional	0	0	4	16282684
192.168.2.148	DESKT	Micros	7	1	8	32621282

	OP-J3DL0JD	oft Windows 10				
192.168.2.163	GYSJEF006	Microsoft Windows 7 Professional	7	1	4	25470186
192.168.2.168	DP001	Microsoft Windows 7 Professional	7	1	6	25470186
192.168.2.188	CENPAVIF3	Microsoft Windows 8	7	1	7	30034775
192.168.2.249	4500	3Com Switch 4500 3.03.02s168p0	0	0	5	30767998

Elaborado por el autor

5.3. Desarrollo y Resultados de las pruebas del esquema de seguridad

5.3.1. Resultados de las pruebas

Security assessment: **Completed Scan**

Computer name: **GOBERGUAYAS\SERVIDOR**

IP address: **192.168.2.4**

Security report name: **GOBERGUAYAS - SERVIDOR (30-08-2017 18-55)**

Scan date: **30/08/2017 18:55**

Security update catalog: **Microsoft Update**

5.3.2. Resultados de escaneo de actualizaciones de seguridad

Problema: Developer Tools, Runtimes, and Redistributables Security Updates

TABLA 54: **Esquema de seguridad de actualizaciones de seguridad de herramientas de desarrollador, tiempos de ejecución y redistribuibles**

Puntaje	ID	Descripción	Severidad máxima
Faltante	MS09-062	Security Update for Microsoft Visual Studio 2008	Low

		Service Pack 1 (KB972222)	
Faltante	MS12-021	Security Update for Microsoft Visual Studio 2008 Service Pack 1 (KB2669970)	Importante
Faltante	MS11-049	Security Update for Microsoft Visual Studio 2008 Service Pack 1 XML Editor (KB2251487)	Importante
Instalada	MS09-062	Security Update for Microsoft Visual Studio 2008 (KB972221)	Low

Elaborado por autores

Problema: Actualizaciones de seguridad de Office

TABLA 55: Esquema de seguridad de actualizaciones de Office

Puntaje	ID	Descripción	Severidad máxima
Faltante	MS09-043	Security Update for Microsoft Office 2003 Web Components for the 2007	Crítico

		Microsoft Office System (KB947318)	
Faltante	3191828	Security Update for Microsoft Office 2007 suites (KB3191828)	Importante
Faltante	2596904	Security Update for Microsoft Office 2007 suites (KB2596904)	Importante
Faltante	MS16-004	Security Update for Microsoft Office 2007 suites (KB2881067)	Importante
Instalada	949426	Microsoft Office Accounting 2008 UK Service Pack 1 (KB949426)	Low
Instalada	937961	Office 2003 Web Components Service Pack 1 for the 2007 Microsoft Office System	Importante
Instalada	949426	Microsoft Office Accounting 2008 US Service Pack 1 (KB949426)	Low

Elaborado por autores

Problema: Actualizaciones de seguridad de SQL Server

TABLA 56: Esquema de seguridad de actualizaciones de sql server

Puntaje	ID	Descripción	Severidad máxima
Faltante	2546951	Microsoft SQL Server 2008 Service Pack 3 (KB2546951)	Importante
Instalada	MS06-061	MSXML 6.0 RTM Security Update (925673)	Crítico

Elaborado por autores

Problema: Actualizaciones de seguridad de Windows

TABLA 57: Esquema de seguridad de actualizaciones de Windows

Problema	Puntaje	ID	Descripción	Severidad máxima
Developer	Faltante	MS09-	Security	Low

Tools, Runtimes, and Redistributables SU		062	Update for Microsoft Visual Studio 2008 Service Pack 1 (KB972222)	
Developer Tools, Runtimes, and Redistributables SU	Faltante	MS12-021	Security Update for Microsoft Visual Studio 2008 Service Pack 1 (KB2669970)	Important e
Developer Tools, Runtimes, and Redistributables SU	Faltante	MS11-049	Security Update for Microsoft Visual Studio 2008 Service Pack 1 XML Editor (KB2251487)	Important e
Developer	Instalada	MS09-	Security	Low

Tools, Runtimes, and Redistributables SU		062	Update for Microsoft Visual Studio 2008 (KB972221)	
Actualizaciones de seguridad de Office	Faltante	MS09-043	Security Update for Microsoft Office 2003 Web Components for the 2007 Microsoft Office System (KB947318)	Crítico
Actualizaciones de seguridad de Office	Faltante	3191828	Security Update for Microsoft Office 2007 suites (KB3191828)	Importante
Actualizacione	Faltante	25969	Security	Important

s de seguridad de Office		04	Update for Microsoft Office 2007 suites (KB2596904)	e
Actualizaciones de seguridad de Office	Faltante	MS16-004	Security Update for Microsoft Office 2007 suites (KB2881067)	Important e
Actualizaciones de seguridad de Office	Instalada	949426	Microsoft Office Accounting 2008 UK Service Pack 1 (KB949426)	Important e
Actualizaciones de seguridad de Office	Instalada	937961	Office 2003 Web Components Service Pack 1 for the 2007	Important e

			Microsoft Office System	
Actualizaciones de seguridad de Office	Instalada	949426	Microsoft Office Accounting 2008 US Service Pack 1 (KB949426)	Importante
SQL Server Security Updates	Faltante	2546951	Microsoft SQL Server 2008 Service Pack 3 (KB2546951)	Importante
SQL Server Security Updates	Instalada	MS06-061	MSXML 6.0 RTM Security Update (925673)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS15-004	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB3019978)	
Actualizaciones de seguridad de Windows	Instalada	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2884256)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-102	Security Update for Windows Server 2008 R2 x64 Edition (KB3084135)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-118	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	Importante

			and Windows Server 2008 R2 SP1 for x64-based Systems (KB3097989)	
Actualizaciones de seguridad de Windows	Instalada	MS14-046	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2943357)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS14-074	Security Update for Windows Server 2008	Importante

			R2 x64 Edition (KB3003743)	
Actualizaciones de seguridad de Windows	Instalada	MS13-079	Security Update for Windows Server 2008 R2 x64 Edition (KB2853587)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-080	Security Update for Windows Server 2008 R2 x64 Edition (KB3078601)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS16-032	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB3139914)	
Actualizaciones de seguridad de Windows	Instalada	MS12-083	Security Update for Windows Server 2008 R2 x64 Edition (KB2765809)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS13-007	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2736422)	Important e
Actualizacione	Instalada	MS12-	Security	Important

s de seguridad de Windows		006	Update for Windows Server 2008 R2 x64 Edition (KB2585542)	e
Actualizaciones de seguridad de Windows	Instalada	890830	Windows Malicious Software Removal Tool x64 - August 2017 (KB890830)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS14-072	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for	Important e

			x64-based Systems (KB2978120)	
Actualizaciones de seguridad de Windows	Instalada	MS14-053	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2973112)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS11-085	Security Update for Windows Server 2008 R2 x64 Edition (KB2620704)	Importante

			Low	
Actualizaciones de seguridad de Windows	Instalada	MS15-028	Security Update for Windows Server 2008 R2 x64 Edition (KB3030377)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS11-075	Security Update for Windows Server 2008 R2 x64 Edition (KB2564958)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS15-037	Security Update for Windows Server 2008 R2 x64 Edition (KB3046269)	Important e

Actualizaciones de seguridad de Windows	Instalada	MS15-085	Security Update for Windows Server 2008 R2 x64 Edition (KB3071756)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS14-064	Security Update for Windows Server 2008 R2 x64 Edition (KB3010788)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS16-072	Security Update for Windows Server 2008 R2 x64 Edition (KB3159398)	Importante
Actualizacione	Instalada	MS15-	Security	Important

s de seguridad de Windows		041	Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB3037574)	e
Actualizaciones de seguridad de Windows	Instalada	MS15-097	Security Update for Windows Server 2008 R2 x64 Edition (KB3086255)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS11-024	Security Update for Windows Server 2008	Important e

			R2 x64 Edition (KB2506212)	
Actualizaciones de seguridad de Windows	Instalada	MS14-066	Security Update for Windows Server 2008 R2 x64 Edition (KB2992611)	Crítico
Actualizaciones de seguridad de Windows	Instalada	3004375	Security Update for Windows Server 2008 R2 x64 Edition (KB3004375)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS16-021	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB3133043)	
Actualizaciones de seguridad de Windows	Instalada	MS13-082	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2861698)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS14-007	Security Update for Windows Server 2008 R2 x64 Edition (KB2912390)	Crítico
Actualizacione	Instalada	MS15-	Security	Important

s de seguridad de Windows		071	Update for Windows Server 2008 R2 x64 Edition (KB3068457)	e
Actualizaciones de seguridad de Windows	Instalada	MS16-055	Security Update for Windows Server 2008 R2 x64 Edition (KB3156016)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS16-019	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for	Important e

			x64 (KB3122648)	
Actualizaciones de seguridad de Windows	Instalada	MS16-055	Security Update for Windows Server 2008 R2 x64 Edition (KB3156019)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS11-030	Security Update for Windows Server 2008 R2 x64 Edition (KB2509553)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS16-014	Security Update for Windows Server 2008 R2 x64 Edition	Importante

			(KB3126587)	
Actualizaciones de seguridad de Windows	Instalada	MS14-078	Security Update for Windows Server 2008 R2 x64 Edition (KB2991963) Moderada	Importante
Actualizaciones de seguridad de Windows	Instalada	MS13-004	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2742599)	Importante
Actualizacione	Instalada	MS14-	Security	Crítico

s de seguridad de Windows		068	Update for Windows Server 2008 R2 x64 Edition (KB3011780)	
Actualizaciones de seguridad de Windows	Instalada	MS12-074	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2729452)	Crítico
Actualizaciones de seguridad de Windows	Instalada	2984972	Security Update for Windows Server 2008	Importante

			R2 x64 Edition (KB2984972)	
Actualizaciones de seguridad de Windows	Instalada	MS15-117	Security Update for Windows Server 2008 R2 x64 Edition (KB3101722)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS16-087	Security Update for Windows Server 2008 R2 x64 Edition (KB3170455)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS14-009	Security Update for Microsoft .NET Framework 3.5.1 on	Importante

			Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2911501)	
Actualizaciones de seguridad de Windows	Instalada	MS12-020	Security Update for Windows Server 2008 R2 x64 Edition (KB2621440)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS15-119	Security Update for Windows Server 2008 R2 x64 Edition (KB3092601)	Importante
Actualizacione	Instalada	MS14-	Security	Important

s de seguridad de Windows		039	Update for Windows Server 2008 R2 x64 Edition (KB2973201)	e
Actualizaciones de seguridad de Windows	Instalada	MS12-035	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2604115)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS12-024	Security Update for Windows Server 2008	Crítico

			R2 x64 Edition (KB2653956)	
Actualizaciones de seguridad de Windows	Instalada	MS15-005	Security Update for Windows Server 2008 R2 x64 Edition (KB3022777)	Importante
Actualizaciones de seguridad de Windows	Instalada	2841134	Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-132	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB3108371)	
Actualizaciones de seguridad de Windows	Instalada	MS12-054	Security Update for Windows Server 2008 R2 x64 Edition (KB2705219)	Moderada
Actualizaciones de seguridad de Windows	Instalada	MS11-059	Security Update for Windows Server 2008 R2 x64 Edition (KB2560656)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-084	Security Update for Windows Server 2008 R2 x64 Edition	Importante

			(KB3076895)	
Actualizaciones de seguridad de Windows	Instalada	MS16-077	Security Update for Windows Server 2008 R2 x64 Edition (KB3161949)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS16-007	Security Update for Windows Server 2008 R2 x64 Edition (KB3108664)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-038	Security Update for Windows Server 2008 R2 x64 Edition (KB3045685)	Importante

Actualizaciones de seguridad de Windows	Instalada	MS13-099	Security Update for Windows Server 2008 R2 x64 Edition (KB2892074)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS15-133	Security Update for Windows Server 2008 R2 x64 Edition (KB3109103)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-024	Security Update for Windows Server 2008 R2 x64 Edition (KB3035132)	Importante
Actualizacione	Instalada	29733	Security	Important

s de seguridad de Windows		51	Update for Windows Server 2008 R2 x64 Edition (KB2973351)	e
Actualizaciones de seguridad de Windows	Instalada	MS12-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2758857)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS15-048	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for	Important e

			x64-based Systems (KB3023215)	
Actualizaciones de seguridad de Windows	Instalada	MS15-088	Security Update for Windows Server 2008 R2 x64 Edition (KB3046017)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-101	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB3074543)	Importante

Actualizaciones de seguridad de Windows	Instalada	MS12-082	Security Update for Windows Server 2008 R2 x64 Edition (KB2770660)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS13-090	Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB2900986)	Moderada
Actualizaciones de seguridad de Windows	Instalada	MS15-060	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB3059317)	
Actualizaciones de seguridad de Windows	Instalada	MS15-132	Security Update for Windows Server 2008 R2 x64 Edition (KB3108381)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2864202)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-082	Security Update for Windows Server 2008 R2 x64 Edition	Importante

			(KB3075220)	
Actualizaciones de seguridad de Windows	Instalada	MS16-007	Security Update for Windows Server 2008 R2 x64 Edition (KB3110329)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS12-073	Security Update for Windows Server 2008 R2 x64 Edition (KB2719033)	Moderada
Actualizaciones de seguridad de Windows	Instalada	4034664	2017-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-	Crítico

			based Systems (KB4034664)	
Actualizaciones de seguridad de Windows	Instalada	MS15-090	Security Update for Windows Server 2008 R2 x64 Edition (KB3060716)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2868038)	Importante
Actualizaciones de seguridad de Windows	Instalada	3042058	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB3042058)	
Actualizaciones de seguridad de Windows	Instalada	MS14-057	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2972100)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS12-012	Security Update for Windows Server 2008 R2 x64 Edition (KB2643719)	Importante
Actualizacione	Instalada	28621	Security	Important

s de seguridad de Windows		52	Update for Windows Server 2008 R2 x64 Edition (KB2862152)	e
Actualizaciones de seguridad de Windows	Instalada	2871997	Security Update for Windows Server 2008 R2 x64 Edition (KB2871997)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS14-053	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for	Important e

			x64-based Systems (KB2972211)	
Actualizaciones de seguridad de Windows	Instalada	MS15-050	Security Update for Windows Server 2008 R2 x64 Edition (KB3055642)	Importante
Actualizaciones de seguridad de Windows	Instalada	2977292	Security Update for Windows Server 2008 R2 x64 Edition (KB2977292)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS12-013	Security Update for Windows Server 2008 R2 x64	Crítico

			Edition (KB2654428)	
Actualizaciones de seguridad de Windows	Instalada	MS15-014	Security Update for Windows Server 2008 R2 x64 Edition (KB3004361	Importante
Actualizaciones de seguridad de Windows	Instalada	MS14-057	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2968294)	Importante
Actualizacione	Instalada	MS12-	Security	Moderad

s de seguridad de Windows		073	Update for Windows Server 2008 R2 x64 Edition (KB2716513)	a
Actualizaciones de seguridad de Windows	Instalada	MS14-046	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2937610)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS14-026	Security Update for Microsoft .NET Framework	Importante

			3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2931356)	
Actualizaciones de seguridad de Windows	Instalada	MS00-000	Security Update for Windows Server 2008 R2 x64 Edition (KB2813430)	Moderada
Actualizaciones de seguridad de Windows	Instalada	MS16-082	Security Update for Windows Server 2008 R2 x64 Edition (KB3161958)	Importante

Actualizaciones de seguridad de Windows	Instalada	4034733	Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB4034733)	Moderada
Actualizaciones de seguridad de Windows	Instalada	2894844	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems	Importante

			(KB2894844)	
Actualizaciones de seguridad de Windows	Instalada	4019112	May, 2017 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Server 2008 R2 for x64 (KB4019112)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-015	Security Update for Windows Server 2008 R2 x64 Edition (KB3031432)	Importante
Actualizacione	Instalada	MS13-	Security	Important

s de seguridad de Windows		052	Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2840631)	e
Actualizaciones de seguridad de Windows	Instalada	MS12-045	Security Update for Windows Server 2008 R2 x64 Edition (KB2698365)	Moderada
Actualizaciones de seguridad de Windows	Instalada	MS12-020	Security Update for Windows Server 2008	Crítico

			R2 x64 Edition (KB2667402)	
Actualizaciones de seguridad de Windows	Instalada	MS12-036	Security Update for Windows Server 2008 R2 x64 Edition (KB2685939)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS16-033	Security Update for Windows Server 2008 R2 x64 Edition (KB3139398)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS13-027	Security Update for Windows Server 2008 R2 x64	Importante

			Edition (KB2807986)	
Actualizaciones de seguridad de Windows	Instalada	MS13-098	Security Update for Windows Server 2008 R2 x64 Edition (KB2893294)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS16-007	Security Update for Windows Server 2008 R2 x64 Edition (KB3109560)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS15-080	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7	Crítico

			SP1 and Windows Server 2008 R2 SP1 for x64 (KB3072305)	
Actualizaciones de seguridad de Windows	Instalada	MS15-003	Security Update for Windows Server 2008 R2 x64 Edition (KB3021674)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS13-015	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for	Importante

			x64-based Systems (KB2789645)	
Actualizaciones de seguridad de Windows	Instalada	MS15-011	Security Update for Windows Server 2008 R2 x64 Edition (KB3000483)	Crítico
Actualizaciones de seguridad de Windows	Instalada	MS12-033	Security Update for Windows Server 2008 R2 x64 Edition (KB2690533)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS16-019	Security Update for Microsoft .NET Framework 3.5.1 on	Importante

			Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3127220)	
Actualizaciones de seguridad de Windows	Instalada	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2862330)	Importante
Actualizaciones de seguridad de Windows	Instalada	MS11-100	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for	Crítico

			x64-based Systems (KB2656356)	
Actualizaciones de seguridad de Windows	Instalada	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2862335)	Important e
Actualizaciones de seguridad de Windows	Instalada	MS15-029	Security Update for Windows Server 2008 R2 x64 Edition (KB3035126)	Important e

Elaborado por autores

5.3.3. Resultados de escaneo de Windows

Vulnerabilidades administrativas

TABLA 58: Resultado de escaneo de Windows

Puntaje	Problema	Resultado
	Password Expiration	Some user accounts (4 of 93) have non-expiring passwords. User Invitado christian.ayala pamela.massay temporal1
	Administrators	More than 2 Administrators were found on this computer. User GOBERGUAYAS\Administrador GOBERGUAYAS\Administradores de empresas GOBERGUAYAS\TIC
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. **Connection Name Firewall Exceptions** **All Connections Off** **Services** **Conexión de área local Off*** **Services***

		Conexión de área local 2 Off* **Services*** **Conexión de área local 3 Off*** **Services***
	Incomplete Updates	No incomplete software update installations were found
	File System	All hard drives (1) are using the NTFS file system. **Drive Letter File System** **C: NTFS**
	Guest Account	The Guest account is disabled on this computer.
	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.
	Automatic Updates	Updates are automatically downloaded and Instalada on this computer.
	Local Account Password Test	Password checks are not performed on a domain controller.

Elaborado por autores

5.3.4. Información adicional del sistema

5.3.4.1. Resultados de escaneo de Internet Information Services (IIS)

TABLA 59: Resultados de Internet Information Services (IIS)

Puntaje	Problema	Resultado
	Sample Applications	IIS sample applications are not Instalada.
	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
	Parent Paths	Parent paths are not enabled.
	MSADC and Scripts Virtual Directories	The MSADC and Scripts virtual directories are not present.
	IIS Lockdown Tool	The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Windows Server 2003 installations

		running IIS 6.0.

TABLA 60: Tabla de resultados

Puntaje	Problema	Resultado
	Domain Controller Test	IIS is running on a primary or backup domain controller
	IIS Logging Enabled	All web and FTP sites are using the recommended logging options.

Elaborado por autores

5.3.4.2. Resultados de escaneo de SQL Server: Instancia (por defecto)

TABLA 61: Resultados de escaneo de SQL Server: Instancia (default)

Puntaje	Problema	Resultado
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.

	Password Policy	Enable password policy and expiration for the SQL server accounts.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	Sysadmins	More than 2 members of sysadmin role are present.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts should not be members of the local Administrators group or run as LocalSystem. **Instance Service Account** **Problema (default)** **MSSQLServer**

		SYSTEM LocalSystem account. (default) SQLServerAgent SYSTEM LocalSystem account.
	CmdExec role	CmdExec is restricted to sysadmin only
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Folder Permissions	**Instance Folder User (default) Internal error. -**
	Sysadmin role members	BUILTIN\Administrators group is not part of sysadmin role.
	Guest Account	The Guest account is not enabled in any of the

		databases.
	SSIS Roles	The BUILTIN Admin does not belong to the SSIS roles.
	Sysdtslog	Sysdtslogs90 table does not exist in the Master or MSDB databases

Elaborado por autores

5.3.4.3. Resultados de escaneo de SQL Server: Instancia MSAS10.MSSQLSERVER

TABLA 62: Resultados de escaneo sql server: instancia msas10.mssqlserver

Puntaje	Problema	Resultado
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL

		Server and/or MSDE and Windows (Mixed Mode).
	CmdExec role	CmdExec is restricted to sysadmin only.
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.

Elaborado por autores

5.3.4.4. Resultados de escaneo de SQL Server: Instancia MSRS10.MSSQLSERVER

TABLA 63: Resultados de escaneo de SQL Server: instancia msrs10.mssqlserver

Puntaje	Problema	Resultado
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	CmdExec role	CmdExec is restricted to sysadmin only.
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry

		keys.
	Folder Permissions	**Instance Folder User MSRS10.MSSQLSERVER Internal error. -**
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.

Elaborado por autores

5.3.4.5. Resultados de escaneo de SQL Server: Instancia MSSQL10.MSSQLSERVER

TABLA 64: Resultados de escaneo SQL Server: Instancia mssql10.mssqlserver

Puntaje	Problema	Resultado
	CmdExec role	Error reading registry. If you are scanning a remote computer the Remote Registry service on that computer should be enabled. (13)
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	Folder Permissions	Permissions on the SQL Server and/or MSDE installation folders are not set properly **Instance** **Folder** **User** **MSSQL10.MSSQLSERVER** **C:\Program Files\Microsoft SQL**

		\CREATOR OWNER **Server\MSSQL10.MSSQLSERVER \MSSQL\Binn** **MSSQL10.MSSQLSERVER** **C:\Program Files\Microsoft SQL** **BUILTIN\Usuarios** **Server\MSSQL10.MSSQLSERVER \MSSQL\Binn** **MSSQL10.MSSQLSERVER** **C:\Program Files\Microsoft SQL** **NT SERVICE\MSSQLSERVER** **Server\MSSQL10.MSSQLSERVER \MSSQL\Binn** **MSSQL10.MSSQLSERVER** **C:\Program Files\Microsoft SQL** **\CREATOR OWNER** **Server\MSSQL10.MSSQLSERVER \MSSQL\Data** **MSSQL10.MSSQLSERVER** **C:\Program Files\Microsoft SQL** **NT SERVICE\MSSQLSERVER** **Server\MSSQL10.MSSQLSERVER \MSSQL\Data** **MSSQL10.MSSQLSERVER** **C:\Program Files\Microsoft SQL**

		GOBERGUAYAS\Mariuxi.cordova **Server\MSSQL10.MSSQLSERVER** **\MSSQL\Data**
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.

Elaborado por autores

5.3.4.6. Resultados de escaneo de SQL Server: Instancia (por defecto) (32-bit)

TABLA 65: Resultados de escaneo SQL Server: Instancia (default) (32-bit)

Puntaje	Problema	Resultado
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	Password Policy	Enable password policy and expiration for the SQL server accounts.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	Sysadmins	More than 2 members of sysadmin role are present.
	Service	SQL Server, SQL Server

	Accounts	Agent, MSDE and/or MSDE Agent service accounts should not be members of the local Administrators group or run as LocalSystem. **Instance Service Account Problema (default) (32-bit) MSSQLServer SYSTEM LocalSystem account.** (default) (32-bit) SQLServerAgent SYSTEM LocalSystem account.
	CmdExec role	CmdExec is restricted to sysadmin only.
	Registry Permissions	The Everyone group does not have more

		than Read access to the SQL Server and/or MSDE registry keys.
	Folder Permissions	**Instance Folder User (default) (32-bit) Internal error. -**
	Sysadmin role members	BUILTIN\Administrators group is not part of sysadmin role.
	Guest Account	The Guest account is not enabled in any of the databases.
	SSIS Roles	The BUILTIN Admin does not belong to the SSIS roles.
	Sysdtslog	Sysdtslogs90 table does not exist in the Master or MSDB databases

Elaborado por autores

5.3.4.7. Resultados de escaneo de aplicaciones de escritorio

TABLA 66: Resultados de escaneo de aplicaciones de escritorio Windows

Puntaje	Problema	Resultado
✓	IE Zones	Internet Explorer zones have secure settings for all users
	Macro Security	No supported Microsoft Office products are Instalada.

Elaborado por autores

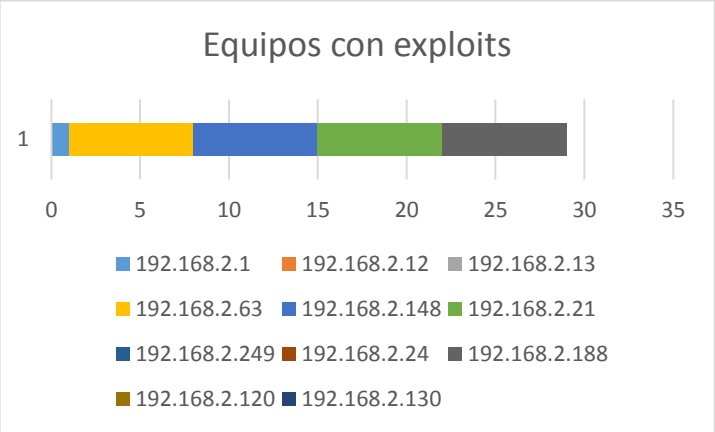


FIGURA 5.38: Equipos con exploits. Fuente: Los autores

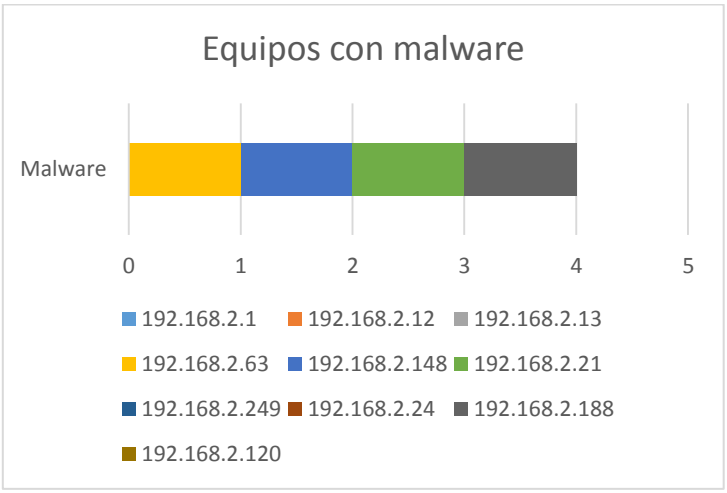


FIGURA 5.39: Equipos con malware. Fuente: Los autores

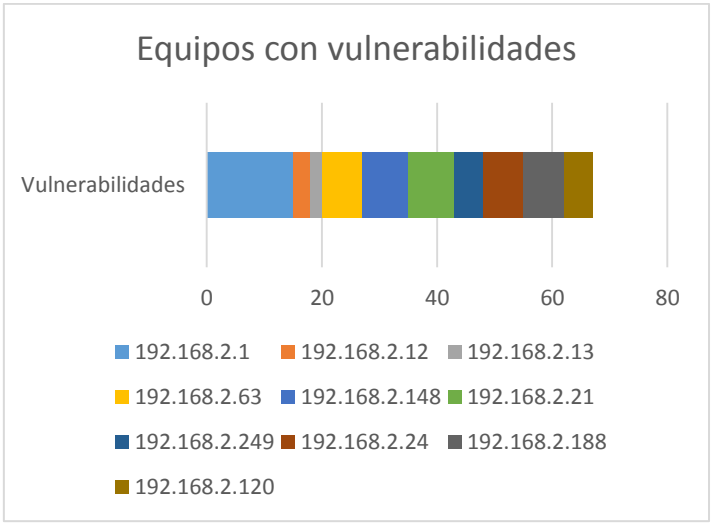


FIGURA 5.40: Equipos con vulnerabilidades. Fuente: Los autores

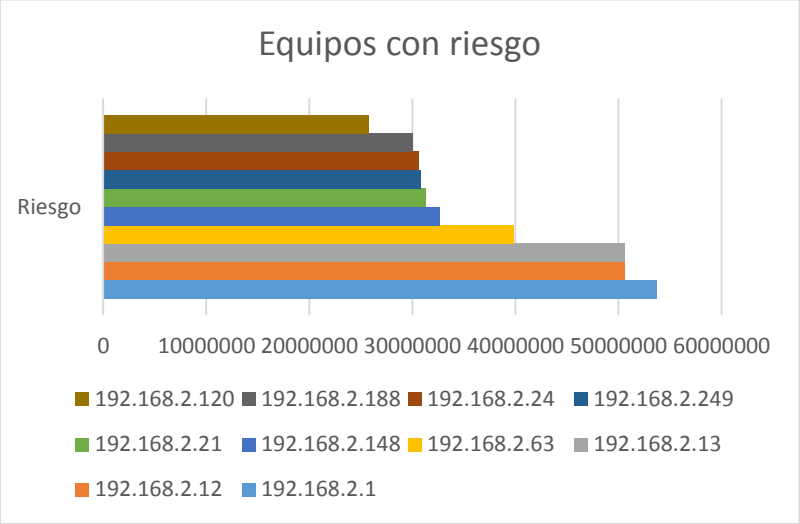


FIGURA 5.41: Equipos con riesgo. Fuente: Los autores

CONCLUSIONES Y RECOMENDACIONES

El trabajo de titulación permitió cumplir con los objetivos detallados en el primer capítulo y se establece las siguientes conclusiones:

1) La Gobernación de la provincia del Guayas implementa una política de seguridad de la información, donde se ha analizado y evaluado los riesgos de los diferentes activos presentados en el proceso de concursos de méritos y oposición.

2) En esta investigación se emplea la metodología de MAGERIT, para conocer las amenazas que se presentan en los activos del

proceso de concursos de méritos y oposición y de esa manera reducir las vulnerabilidades presentes.

3) Para llevar el control de la seguridad de la información se utilizó la herramienta MSBA 2.3 (Microsoft Baseline Security Analyzer) y Rapid7 insight en donde se realizó la evaluación de la actualizaciones de los equipos Windows que se encuentran en dominio de la gobernación, los parches de seguridad y de aplicaciones Windows, y demás vulnerabilidades que se detallan en el trabajo de titulación.

4) Para reducir la probabilidad de que se presente incidentes, se debe especificar un proceso de notificaciones de alertas de incidentes donde todos los funcionarios involucrados lo conozcan con claridad para que puedan actuar cuando reconozcan un problema.

5) Se establece políticas de medios de almacenamiento de información, para evitar el robo, daño o acceso no autorizado.

6) Documentar las reglas de acceso a los activos de la información, estableciendo políticas y procedimiento para uso de la información. Limitando la asignación de privilegios en los controles de accesos.

7) En la gobernación del guayas como en las demás instituciones públicas del ecuador se han presentados incidentes en la seguridad de la información que han generado desconfianza en la población, y se determina que una de las principales causas es la falta de controles, normas y policitas que protejan la información

8) Al finalizar el proceso de concurso de mérito y oposición se recomienda se realice una metodología de evaluación para asegurar el buen manejo de la información del proceso.

9) Por medio de esta investigación se ha podido determinar la madurez de la información con respecto a la seguridad de la información basada en la norma ISO 27001.

10) El departamento de tecnología de la información y comunicación debe estar pendiente que las políticas establecidas se encuentren 100% funcional durante todo el proceso de concurso de mérito y

oposición para que no exista fuga de la información documentando los análisis de gestión y control de la seguridad de la información.

Se detalla a continuación las recomendaciones brindadas a la Gobernación de la provincia del Guayas:

1) Dar el menor privilegio. Cualquier usuario, programa, administrador, sistema, etc. debe tener sólo los privilegios necesarios para cumplir de manera adecuada su tarea y nada más.

2) La cadena se rompe por el eslabón más débil. El máximo grado de seguridad en todo sistema de seguridad no es la suma de todo el conjunto de medidas sino el grado de seguridad de su eslabón más débil

3) Defensa en profundidad. La seguridad de un sistema no debe depender de un solo método de seguridad por muy fuerte que sea éste, sino que es necesario establecer varios métodos sucesivos de seguridad.

4) Establecer un punto de control centralizado. Donde se establece un único punto de acceso a un sistema, para que así cuando algún

atacante quiera intentar acceder a este tenga que pasar por ese punto. No quiere decir que se esté utilizando un solo método de seguridad, sino que se alinean todos los mecanismos de seguridad para que el usuario ingresa por ellos para tener acceso al sistema.

5) Seguridad no equivale a oscuridad. Un sistema no es más seguro porque se esconde sus defectos y vulnerabilidades, sino porque lo conocemos y corregimos estableciendo medidas de seguridad adecuadas.

6) Seguridad en caso de falla. En el momento de que cualquier método de seguridad falle, el sistema debe quedar en un estado seguro.

7) Participación universal. La participación voluntaria de todos los usuarios en la seguridad de un sistema es el método más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.

8) Participación de simplicidad: Mantener las cosas simples, las hace más fáciles de comprender. Si no se entiende algo, difícilmente

puede saberse si es seguro y; la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

9) Elaborar un análisis de riesgo es laborioso y costoso

10) Desarrollar un mapa de activos y valorarlos requiere de la participación y colaboración de muchos perfiles dentro de la organización.

11) Se debe lograr una uniformidad de criterio entre todos

12) Es Importante cuantificar los riesgos, pero más Importante aún es relativizarlos, debido que en un análisis de riesgos aparecen multitud de datos.

13) La única forma de afrontar la complejidad es centrarse en lo más Importante (máximo impacto, máximo riesgo)

14) Pero si los datos no están bien ordenados en términos relativos, su interpretación es imposible

15) Solo puede mejorarse aquello que se controla y sólo puede controlarse aquello que es medido.

BIBLIOGRAFÍA

[1] DIAZ, A. (2 de 12 de 2010). *Seguridad y privacidad info* . Recuperado el 2 de 1 de 2017, de Seguridad y privacidad info : http://seguridadyprivacidadinfo.blogspot.com/p/ataques-comunes-una-red-lan.html

[2] Dirección General de Modernización Administrativa, p. e. (2012). *MARGERIT - Versión 3.0 Metodología de anáisis y gestión de riesgo de los sistemas de información Libro III - Guía de Técnicas .* España: Administración electronica.

[3] Dirección General de modernización administrativa, p. e. (2012). *MARGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgo de los sistemas de información Libro I - Método.* ESPAÑA: Administración electronica.

[4] Dirección General de Modernización, p. e. (2012). *MARGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información Libro II - Catalogo de elementos.* España: Administración electronica.

[5] DUARTE, E. (11 de 07 de 2012). *CAPACITY Informacion Technology Academy*. Recuperado el 04 de 03 de 2017, de CAPACITY Informacion Technology Academy: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

[6] Erb, M. (octubre de 2008). *Gestión de Riesgo en la Seguridad Informática*. (M. Erb, Editor) Recuperado el 19 de diciembre de 2016, de protejete: https://protejete.wordpress.com/

[7] ESPOL. (2009). *dspace ESPOL*. Recuperado el 22 de marzo de 2017, de DSPACE: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/30152/aplicaci%c3%93n%20de%20la%20metodolog%c3%8da%20scrum%20para%20implementar%20el%20esquema%20gubernamental%20de%20seguridad%20de%20la%20informaci%c3%93n%20orientado%20a%20servicios%20tecn

[8] Geier, E. (09 de 05 de 2014). *CIO PERU*. Recuperado el 23 de 01 de 2017, de CIO PERU: https://cioperu.pe/articulo/15863/6-escaneres-de-vulnerabilidades-de-red-gratuitos/

[9] Huerta, A. V. (julio de 2005). *shutdown*. Recuperado el 21 de febrero de 2017, de shutdown: http://www.shutdown.es/

[10] Prpic, M. (Ed.). (6 de 6 de 2010). *redhat*. Recuperado el 12 de 9 de 2016, de redhat: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/6.0_Release_Notes/index.html

[11] Sarquis, C. (8 de octubre de 2012). *SEGURIDAD INFORMATICA*. (C. Sarquis, Editor) Recuperado el 6 de enero de 2017, de blogspot: http://seguridadinformatica-

umex.blogspot.com/p/1.htmlhttp://seguridadinformatica-umex.blogspot.com/p/1.html

[12] Symantec, C. (2017). *ISTR 22: Extraordinary Attacks, High-Dollar Heists, Electoral Disruption.* California: Symantec.

[13] Villalón Huerta, A. (Julio de 2002). *SEGURIDAD EN UNIX Y REDES.* Obtenido de Red IRIS: https://www.rediris.es/cert/doc/unixsec/

[14] Manual de diagramación de procesos bajo estándar BPMN-ANALITICA. Obtenido de Analítica: http://www.analitica.com.co/website/images/stories/documentosTecnicos_SGP/Manual%20de%20Diagramacion%20de%20Procesos%20Bajo%20Estandar%20BPMN.pdf

GLOSARIO

TERMINOS DEL PROCESO

Administrador del concurso: Servidor de la institución del Estado que es designado por el responsable de la UATH.

Análisis del Puesto: Es el proceso mediante el cual se verifica el cumplimiento de la hoja de vida.

Banco de elegibles: Es el registro de los postulantes en un concurso de méritos y oposición, que superaron la etapa del mérito y las pruebas de conocimientos técnicos y psicométricas.

Banco de preguntas: Es el listado de preguntas con sus respuestas, del cual se va a seleccionar aleatoriamente las preguntas para definir un cuestionario que se aplicará en la prueba de conocimientos técnicos.

Candidato elegible: Aspirante a ingresar a una institución del Estado que ha participado en concurso de méritos y oposición y que superó la etapa de méritos y las pruebas de conocimientos técnicos y psicométricas.

Concurso de méritos y oposición: Proceso por el cual se selecciona a la persona más idónea que reúna los requisitos del perfil del puesto para que ocupe ese puesto con nombramiento permanente luego de haber superado el período de prueba.

Concurso desierto: Es el concurso de méritos y oposición que una vez verificada la ocurrencia de una causal prevista en la Norma Técnica y previa declaratoria del Tribunal de Méritos y Oposición, concluye sin que se determine un ganador y conlleva la facultad de que la institución del Estado lo vuelva convocar.

Convocatoria: La difusión plena del concurso por medio de la plataforma tecnológica, haciendo conocer a la comunidad, la información del proceso de selección para llenar un puesto vacante.

Cronograma: Es el calendario de trabajo o de actividades ordenadas.

Elegibles inmediatos: Son los 5 mejores postulantes de un concurso de méritos y oposición que rindieron las pruebas de conocimientos técnicos, psicométricas y la entrevista, y alcanzaron un puntaje mínimo de 70/100 en el puntaje final, excluyendo a la o el ganador.

Mérito: Es la etapa del concurso en la cual se evalúa el cumplimiento del postulante sobre el perfil del puesto, de acuerdo a la información subida por él a la plataforma tecnológica.

Nombramiento provisional de prueba: Es el acto administrativo por el que se formaliza la relación jurídica laboral entre una institución del Estado y el ganador de un concurso de méritos y oposición (tiene un período de vigencia de 3 meses antes de otorgar el nombramiento permanente y en el caso de ascenso 6 meses).

Oposición: Es el proceso de medición objetiva de los niveles de competencias que ostentan los postulantes a través de pruebas psicométricas, de conocimientos técnicos y de las entrevistas.

Postulación: Es el acto mediante el cual una persona, libre y voluntariamente, durante la difusión de la convocatoria de un concurso de méritos y oposición, manifiesta su interés en participar en el concurso y registra en la plataforma tecnológica la información de su perfil.

Potenciales elegibles: Son los postulantes que en las pruebas de conocimientos técnicos y psicométricas hubieren obtenido setenta (70/100) puntos o más, pero no llegaron a la etapa de entrevistas.

Proceso: Actividad o grupo de actividades que emplean insumos o entradas para transformarlas en salidas como productos o servicios a un cliente externo o interno.

Prueba de conocimientos técnicos: Es el examen escrito elaborado de forma específica y con la complejidad relacionada con el perfil del puesto materia del concurso, que sirve para medir si las y los postulantes al puesto, poseen los conocimientos técnicos que se requieren para desempeñarse en el mismo.

Pruebas psicométricas: Es el conjunto de pruebas psicológicas que miden diversas facetas de la personalidad con el fin de hacer un diagnóstico diferenciado del predominio de una o varios aspectos en una persona.

Servidor/a: Son todas las personas que en cualquier forma o a cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad del sector público.

Tribunal de apelaciones: Es el órgano encargado de conocer y resolver las apelaciones que se presenten por parte de las y los servidores en la etapa de mérito y sobre el Resultados de las pruebas de conocimientos técnicos.

Tribunal de méritos y oposición: Es el órgano encargado, entre otras facultades previstas de declarar a la o el ganador de un concurso de méritos y oposición o declarar desierto el mismo.

TERMINOLOGIA TÉCNICA

Activos: Bienes o recursos que contiene una empresa.

Amenazas: Posible peligro a una situación o afectación malicioso a un activo. Confidencialidad: Propiedad de la información que garantiza el acceso por parte de las personas autorizadas.

Controles: Acción para atenuar un riesgo.

Datos: Contenido digital que contiene información ya sea cualitativa o cuantitativa.

Disponibilidad: Característica que indica está utilizable un servicio.

Fiabilidad: Probabilidad de que se cumpla una función específica y bajo condiciones durante un tiempo determinado.

Gusanos: Malware que se duplica maliciosamente en un activo informático.

Hardware: Elemento físico de un computador o sistema informático.

Hoax: intento de hacer creer que algo falso es real

Impacto: Conjunto de sucesos que se producen en un activo.

Integridad: Es la exactitud de la información o contenido.

No Repudio: Irrefutabilidad de pruebas de partes del emisor de la información.

Ramsomware: Programa que da a la ciberdelincuencia el control de toda nuestra información almacenada en el computador.

Riesgo: Probabilidad de que ocurra un incidente que afecte un activo.

Seguridad informática: Ausencia de Riesgo informáticos.

Software: Programas que permiten a un computador cumplir sus tareas.

Spam: Mensaje no solicitados de remitente desconocidos.

Spyware: Malware o amanezca cibernética que recopila información de un dispositivo para luego ser enviado a una persona externa sin el consentimiento del dueño del dispositivo.

Troyanos: Software malicioso que afecta la seguridad de un activo.

Virus: Programa malicioso que agrava la funcionabilidad de una computadora.

Vulnerabilidad: Capacidad de resistencia a un peligro o riesgo.

BPMN: Business Process Model and Notation, en español Modelo y Notación de Proceso de Negocio, forma gráfica de representar los procesos de negocio, en formato de flujo de trabajo (workflow).

CIS: Center for Internet Security. Centro para la Seguridad de internet. Organización sin fines de lucro cuya misión es identificar, promover, desarrollar, validar y prolongar las soluciones de mejores prácticas para la ciber defensa.

DISA: Defense Information Systems Agency. Agencia de defensa de los sistemas de información. Ente que publica las guías técnicas de implementación de seguridad.

INM: Instituto Nacional de la Meritocracia.

LOSEP: Ley Orgánica del Servicio Público.

MBSA: Microsoft Baseline Security Analyzer (Analizador de Seguridad de línea de base de Microsoft), programa que ayuda a revisar los parches de seguridad y actualizaciones en sistemas operativos Windows y en aplicaciones ofimáticas como Word, Excel, Access, SQL.

MDT: Ministerio del Trabajo.

PEO: Procedimientos estándar de operación.

PHVA: Ciclo Planificar-Hacer-Verificar-Actuar. Herramienta de gestión para mejora continua, constante y progresiva.

SGSI: Sistema de Gestión de la Seguridad de la Información. Concepto principal sobre el que se conforma ISO 27001.

SIITH: Sistema Integrado de Información del Talento Humano.

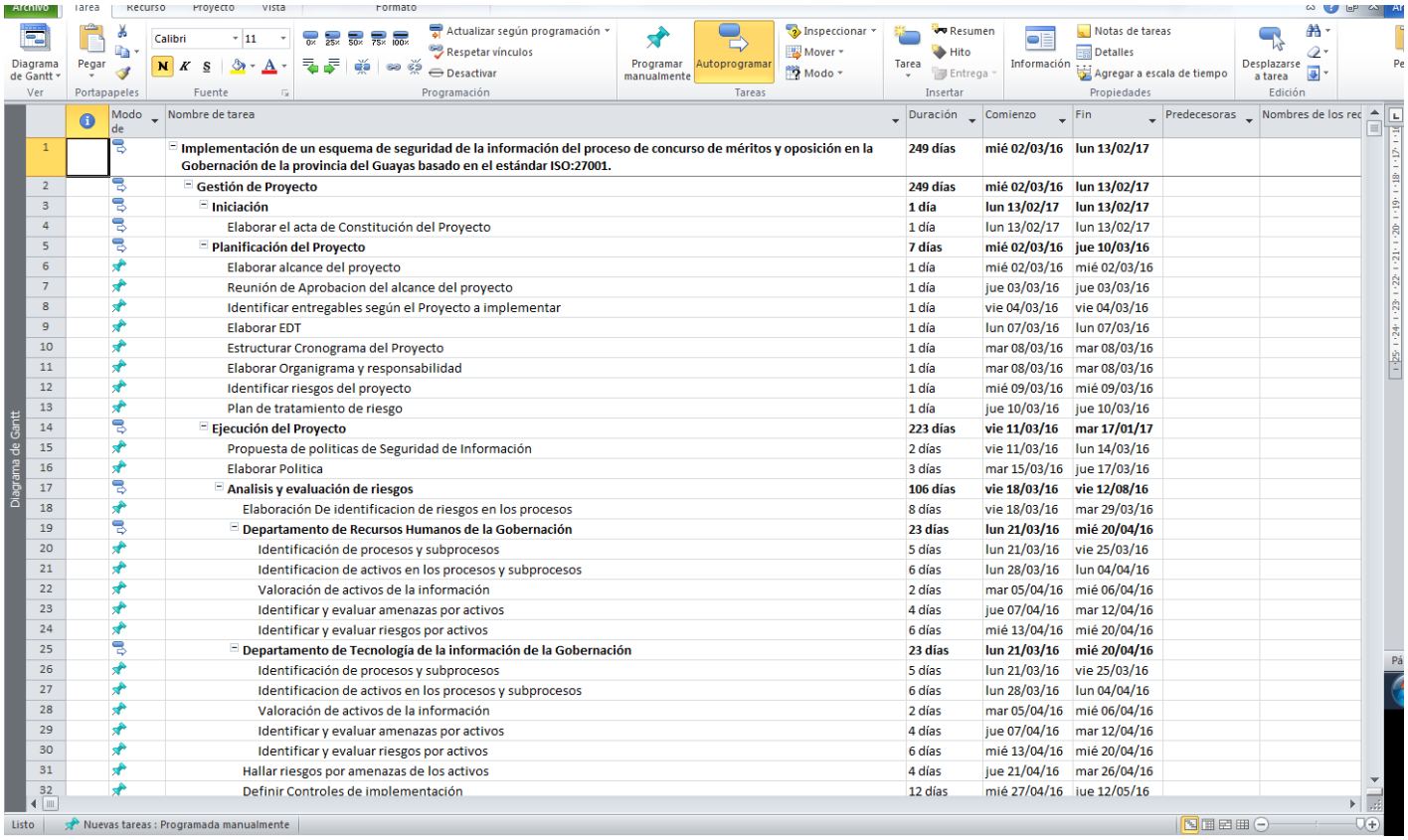
STIG: Security Technical Implementation Guide. Guía Técnica de implementación de seguridad. Metodología de la ciberseguridad para estandarizar protocolos de seguridad en las redes, servidores, computadoras, y diseños lógicos para mejorar la seguridad. Estas guías, cuando son implementadas, mejoran la seguridad de las arquitecturas de software, hardware, físicas y lógicas para reducir las vulnerabilidades.

UATH: Unidad de Administración del Talento Humano.

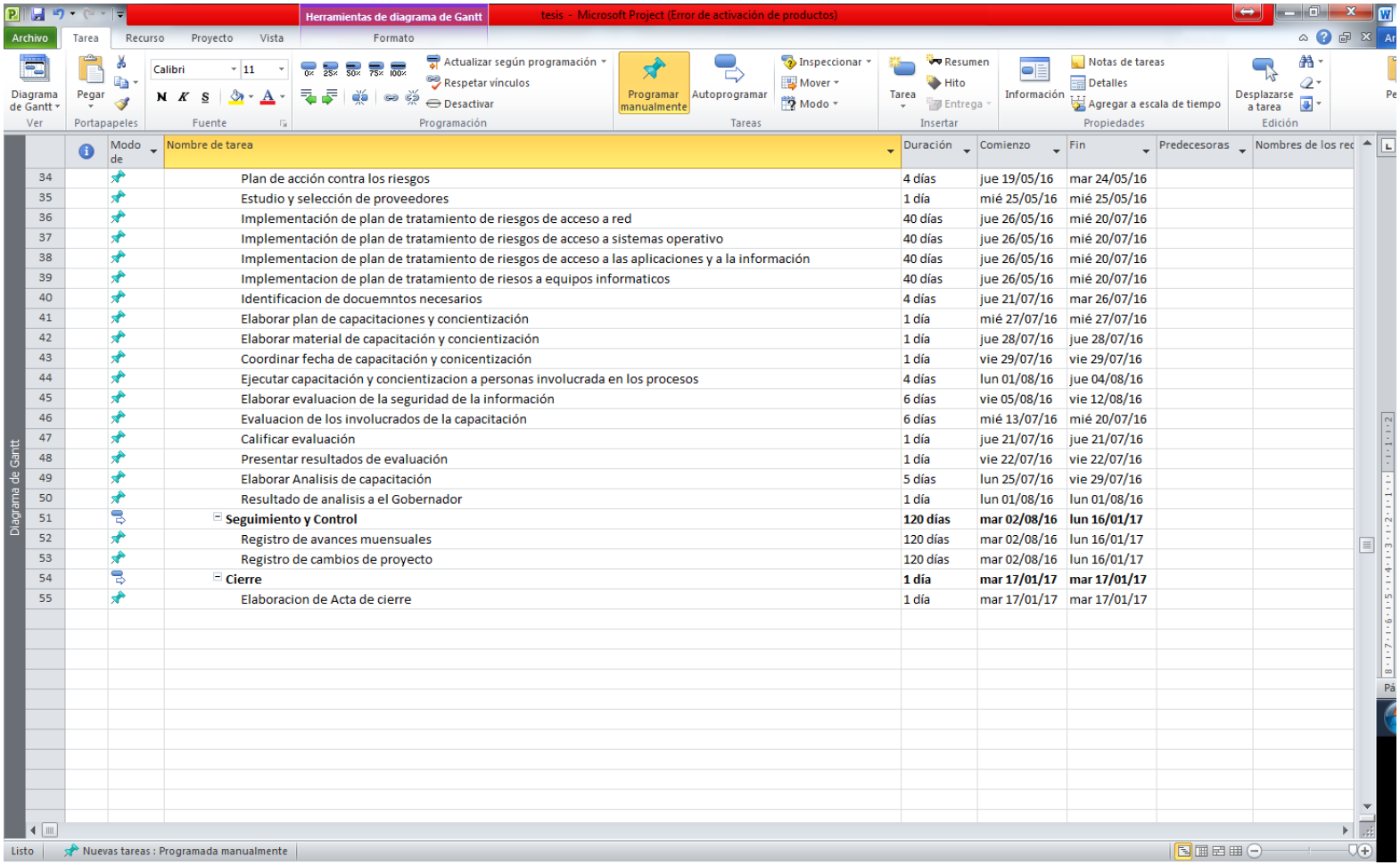
UTIC: Unidad de tecnología de la información y la comunicación.

ANEXOS

ANEXO 1



	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los rec
1		**Implementación de un esquema de seguridad de la información del proceso de concurso de méritos y oposición en la Gobernación de la provincia del Guayas basado en el estándar ISO:27001.**	**249 días**	**mié 02/03/16**	**lun 13/02/17**		
2		**Gestión de Proyecto**	**249 días**	**mié 02/03/16**	**lun 13/02/17**		
3		**Iniciación**	**1 día**	**lun 13/02/17**	**lun 13/02/17**		
4		Elaborar el acta de Constitución del Proyecto	1 día	lun 13/02/17	lun 13/02/17		
5		**Planificación del Proyecto**	**7 días**	**mié 02/03/16**	**jue 10/03/16**		
6		Elaborar alcance del proyecto	1 día	mié 02/03/16	mié 02/03/16		
7		Reunión de Aprobacion del alcance del proyecto	1 día	jue 03/03/16	jue 03/03/16		
8		Identificar entregables según el Proyecto a implementar	1 día	vie 04/03/16	vie 04/03/16		
9		Elaborar EDT	1 día	lun 07/03/16	lun 07/03/16		
10		Estructurar Cronograma del Proyecto	1 día	mar 08/03/16	mar 08/03/16		
11		Elaborar Organigrama y responsabilidad	1 día	mar 08/03/16	mar 08/03/16		
12		Identificar riesgos del proyecto	1 día	mié 09/03/16	mié 09/03/16		
13		Plan de tratamiento de riesgo	1 día	jue 10/03/16	jue 10/03/16		
14		**Ejecución del Proyecto**	**223 días**	**vie 11/03/16**	**mar 17/01/17**		
15		Propuesta de politicas de Seguridad de Información	2 días	vie 11/03/16	lun 14/03/16		
16		Elaborar Politica	3 días	mar 15/03/16	jue 17/03/16		
17		**Analisis y evaluación de riesgos**	**106 días**	**vie 18/03/16**	**vie 12/08/16**		
18		Elaboración De identificacion de riesgos en los procesos	8 días	vie 18/03/16	mar 29/03/16		
19		**Departamento de Recursos Humanos de la Gobernación**	**23 días**	**lun 21/03/16**	**mié 20/04/16**		
20		Identificación de procesos y subprocesos	5 días	lun 21/03/16	vie 25/03/16		
21		Identificacion de activos en los procesos y subprocesos	6 días	lun 28/03/16	lun 04/04/16		
22		Valoración de activos de la información	2 días	mar 05/04/16	mié 06/04/16		
23		Identificar y evaluar amenazas por activos	4 días	jue 07/04/16	mar 12/04/16		
24		Identificar y evaluar riesgos por activos	6 días	mié 13/04/16	mié 20/04/16		
25		**Departamento de Tecnología de la información de la Gobernación**	**23 días**	**lun 21/03/16**	**mié 20/04/16**		
26		Identificación de procesos y subprocesos	5 días	lun 21/03/16	vie 25/03/16		
27		Identificacion de activos en los procesos y subprocesos	6 días	lun 28/03/16	lun 04/04/16		
28		Valoración de activos de la información	2 días	mar 05/04/16	mié 06/04/16		
29		Identificar y evaluar amenazas por activos	4 días	jue 07/04/16	mar 12/04/16		
30		Identificar y evaluar riesgos por activos	6 días	mié 13/04/16	mié 20/04/16		
31		Hallar riesgos por amenazas de los activos	4 días	jue 21/04/16	mar 26/04/16		
32		Definir Controles de implementación	12 días	mié 27/04/16	jue 12/05/16		



	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los rec
34		Plan de acción contra los riesgos	4 días	jue 19/05/16	mar 24/05/16		
35		Estudio y selección de proveedores	1 día	mié 25/05/16	mié 25/05/16		
36		Implementación de plan de tratamiento de riesgos de acceso a red	40 días	jue 26/05/16	mié 20/07/16		
37		Implementación de plan de tratamiento de riesgos de acceso a sistemas operativo	40 días	jue 26/05/16	mié 20/07/16		
38		Implementacion de plan de tratamiento de riesgos de acceso a las aplicaciones y a la información	40 días	jue 26/05/16	mié 20/07/16		
39		Implementacion de plan de tratamiento de riesos a equipos informaticos	40 días	jue 26/05/16	mié 20/07/16		
40		Identificacion de docuemntos necesarios	4 días	jue 21/07/16	mar 26/07/16		
41		Elaborar plan de capacitaciones y concientización	1 día	mié 27/07/16	mié 27/07/16		
42		Elaborar material de capacitación y concientización	1 día	jue 28/07/16	jue 28/07/16		
43		Coordinar fecha de capacitación y conicentización	1 día	vie 29/07/16	vie 29/07/16		
44		Ejecutar capacitación y concientizacion a personas involucrada en los procesos	4 días	lun 01/08/16	jue 04/08/16		
45		Elaborar evaluacion de la seguridad de la información	6 días	vie 05/08/16	vie 12/08/16		
46		Evaluacion de los involucrados de la capacitación	6 días	mié 13/07/16	mié 20/07/16		
47		Calificar evaluación	1 día	jue 21/07/16	jue 21/07/16		
48		Presentar resultados de evaluación	1 día	vie 22/07/16	vie 22/07/16		
49		Elaborar Analisis de capacitación	5 días	lun 25/07/16	vie 29/07/16		
50		Resultado de analisis a el Gobernador	1 día	lun 01/08/16	lun 01/08/16		
51		**Seguimiento y Control**	**120 días**	**mar 02/08/16**	**lun 16/01/17**		
52		Registro de avances muensuales	120 días	mar 02/08/16	lun 16/01/17		
53		Registro de cambios de proyecto	120 días	mar 02/08/16	lun 16/01/17		
54		**Cierre**	**1 día**	**mar 17/01/17**	**mar 17/01/17**		
55		Elaboracion de Acta de cierre	1 día	mar 17/01/17	mar 17/01/17		

ANEXO 2

3com

3Com® SuperStack® 3 Switch 4400 Family

DATA SHEET

Enterprise class manageable 10/100 layer 2/4 switches. Available in 24 and 48-port models with Gigabit connectivity, these switches provide resiliancy, flexibility, plus advanced security and traffic control features.

OVERVIEW

The award-winning 3Com® SuperStack® 3 Switch 4400 family switches provide wirespeed 10/100 Fast Ethernet connectivity with a choice of Gigabit downlinks and are specifically designed for Enterprise workgroup environments. Available in 24 and 48-port models covering important network interface types including Power over Ethernet(PoE), and 100BASE-LX10, with two Gigabit module slots on every unit, these switches display resiliency, flexibility in deployment, and advanced security features. The SuperStack 3 Switch 4400 Family also boasts advanced Quality of Service features that can reduce the latency of packets through the network, with specific traffic prioritization improving the delivery of converged data such as voice and high quality video over IP. Supported by 3Com Global Services and 3Com's outstanding Limited Lifetime Warranty, these switches are ideal for enterprises wanting flexible, resiliant, manageable and secure networks.

KEY BENEFITS

ADVANCED SECURITY

The Switch 4400 family provides advanced security features for network data and management traffic.

User network login with IEEE 802.1X and RADIUS, combined with RADIUS Authenticated Device Access (RADA), provides secure flexible network access control at the edge of the network. Local authentication for up to 50 IEEE 802.1X users and RADA devices offers added flexibility in the absence of a centralized RADIUS server, and supplies a backup solution in case of server failure or connectivity issues.

Authenticated users can be placed automatically into a specific VLAN, creating an even more secure network environment. The Private Ports feature can isolate edge ports to ensure user privacy. Access Control Lists (ACLs) allow or deny traffic based on specific subnet, or individual IP address. SNMP v3 secure encrypted management, Secure Shell (SSH), management VLAN, and management station "trusted IP address" lists help protect the network from rogue management threats.

RESILIANT NETWORKING

Hot-swappable stacking of up to eight units, or 384 10/100 ports, allows for scalable site expansion with continuous operation. Stack-wide link aggregation (LACP) enables high-performance connectivity of up to 4Gbps to the core of the network in a single aggregated link, with ports on different units for added resiliency to maximize network availability.

KEY BENEFITS
(CONTINUED)

NETWORK CONTROL

Network management is available through an embedded web and command line interface (CLI), or via an SNMP management station. Supported by the range of 3Com management offerings including 3Com Network Supervisor.

MULTILAYER TRAFFIC SHAPING

Advanced Multilayer packet classification enables prioritization of mission critical traffic and real-time applications, while freeing bandwidth by eliminating unwanted protocols and applications from the network. Through network login profiles, classification can be dynamically assigned on a per-user basis. Port based rate-limiting enables the maximum bandwidth on each port to be limited, allowing maximum control of network resources while maintaining the full benefit of the powerful traffic prioritization features.

EASY SETUP AND CONFIGURATION

The switches automatically select the optimal speed and duplex mode of connected cables to prevent mis-configuration of the network. They also detect and adjust to cross-over or straight-through cable connections—a feature called auto MDI/MDIX—eliminating the need for specific cables.

WARRANTY

Limited Lifetime Warranty, with Advance Hardware Replacement. See www.3com.com/warranty for details.

SERVICE

3Com products are backed by 3Com Global Services and authorized partners with demonstrated expertise in network assessment, implementation, and maintenance. Ask about 3Com's Network Health Check, installation services, and maintenance service packages available in your area.

Tolly Certified: Layer 2/4 Fast Ethernet Switch Performance Evaluation and Layer 2 Interoperability.

For details, see **www.3com.com/other/pdfs/products/en_US/ss4400_tolly.pdf** and **www.3com.com/ other/ pdfs/products/en_US/tolly_test_4400.pdf**, respectively.

Tolly Verified for Switch Interoperability.

For details, see **www.tolly.com/TVDetail.aspx?ProductID=93**

FEATURES

Performance	
Switching Capacity	24-port models, 8.8 Gbps; 48-port model, 13.6 Gbps
Forwarding Rate	24-port models, 6.6 Mpps; 48-port model, 10.1 Mpps
Store-and-Forward Switching	Latency <2.6 µs
Layer 2 Switching	
MAC Address	8K MAC addresses Secure MAC addresses (256 addresses)
VLAN	64 VLANs (IEEE 802.1Q)
Link Aggregation	IEEE 802.3ad (LACP) Four trunk groups (up to four ports in each) Link Aggregation across stack
Auto-negotiation	Auto-negotiation of port speed, duplex, and connection (MDI/MDIX)
Traffic Control	IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex Broadcast Storm Suppression (3,000 pps threshold)
Spanning Tree	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) • Fast-start mode • Spanning tree enable/disable per port
Multicast Snooping	IGMP v1, v2, and v3 snooping IGMP Querier Filtering for 128 multicast groups
Stacking	
Stacking	Up to 384 ports Single IP address for stack management Resilient stacking (T-type) connectors Hot-swappable
Convergence	
Priority Queues	Four hardware queues per port Strict priority queuing Weighted Round Robin queuing
Traffic Prioritization	CoS Marking / Remarking IEEE 802.1p to DSCP mapping Auto classification of 3Com NBX® telephony traffic Priority based on: • IEEE 802.1p CoS • DSCP (DiffServ Code Point) • TCP/UDP source or destination port number • Default port priority • IP Address / Protocol
Traffic Shaping	Egress rate limiting, port-based: • 1 Mbps increments (10/100 ports) • 8 Mbps increments (Gigabit ports) Application and protocol blocking
Security	
Network Access and User Security	IEEE 802.1X user authentication • RADIUS authentication • Advanced security by locking a port to the MAC address of the authenticated user • Automatically assign VLANs and QoS profile to a port based on user • Guest VLAN option RADIUS Authenticated Device Access (RADA) • Authenticate devices based on MAC address against a RADIUS server • Authenticate multiple devices per port • Automatically assign VLANs and QoS to a port specific to the devices attached • Operates alongside IEEE 802.1X authentication to ensure user and device are allowed access • Local authentication for up to fifty IEEE 802.1X users and RADA devices in absence of a centralized RADIUS server • RADA "whitelist" support enhances flexibility for IEEE 802.1X/RADA deployment • Option to allow default VLAN access when RADIUS server is unavailable

FEATURES (CONTINUED)

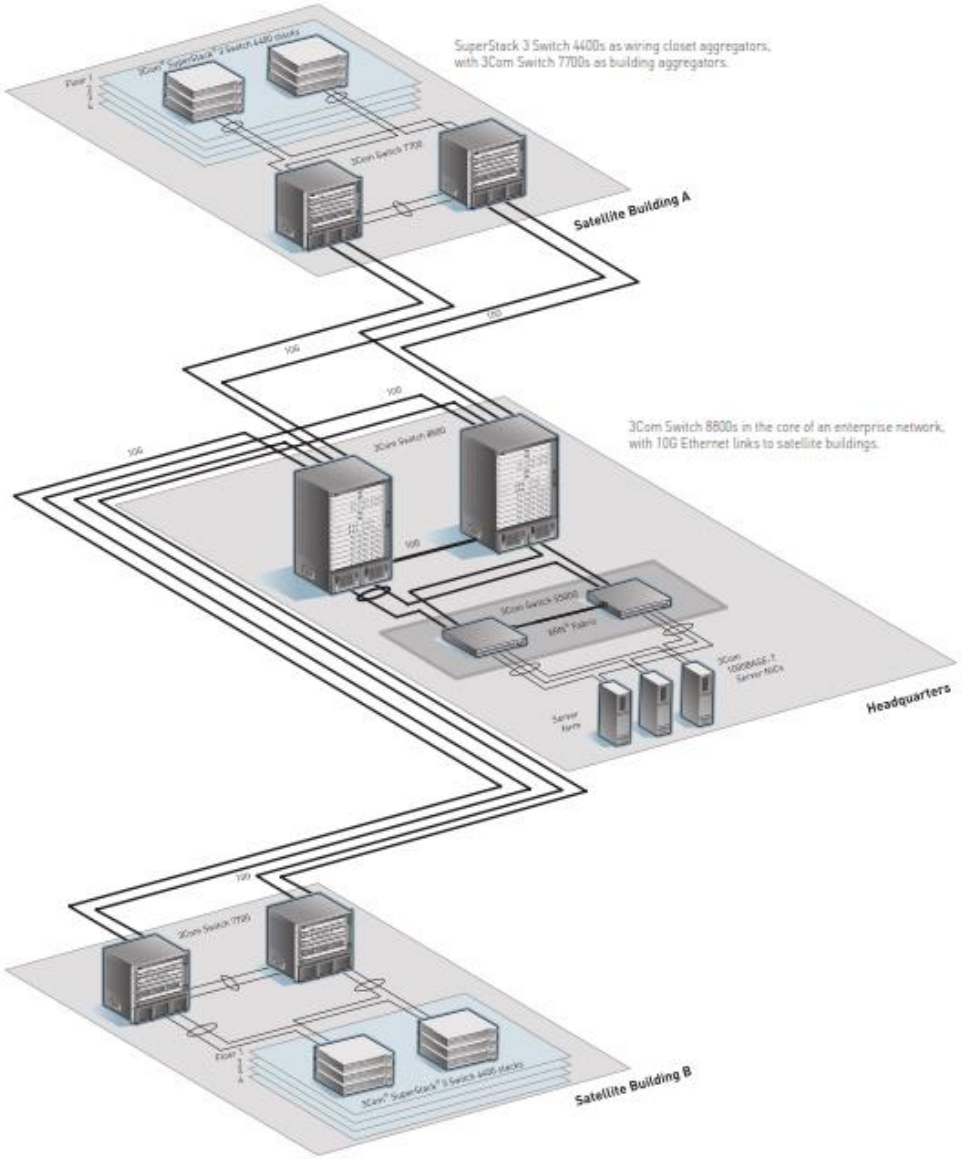
	Disconnect Unknown Device (DUD) Access Control Lists (ACLs) allow or deny traffic based on specific subnet or individual IP address Private Ports feature isolates edge ports at layer 2 to ensure user privacy.
Switch Management	Local or RADIUS management of switch passwords Trusted IP Management Addresses Syslog Telnet • SSH v2 (56 bit or 168 bit DES)
Management	
Remote Management	SNMP v1, SNMP v2, SNMP v3 secure encrypted management User-selectable management VLAN
Software	Backup and restore TFTP configuration: upload/download TFTP agent: upload
Configuration	Command line Serial (9-pin, D-type connector) Telnet Web-based SNMP
Mirror Port / RAP (Roving Analysis Port)	One-to-one
RMON (Remote Monitoring)	Four groups: statistics, history, alarm, and events
IP Address Allocation	DHCP BootP Manual Auto IP
Network Time	Simple Network Time Protocol (SNTP) for time stamp of events captured via Syslog
Management Software	3Com Network Supervisor (copy provided with product) • Topology discovery • Change management reporting • Capacity planning • Event logging • Fault identification and troubleshooting • Utilization monitoring

OPTIONAL SERVICE AND SUPPORT

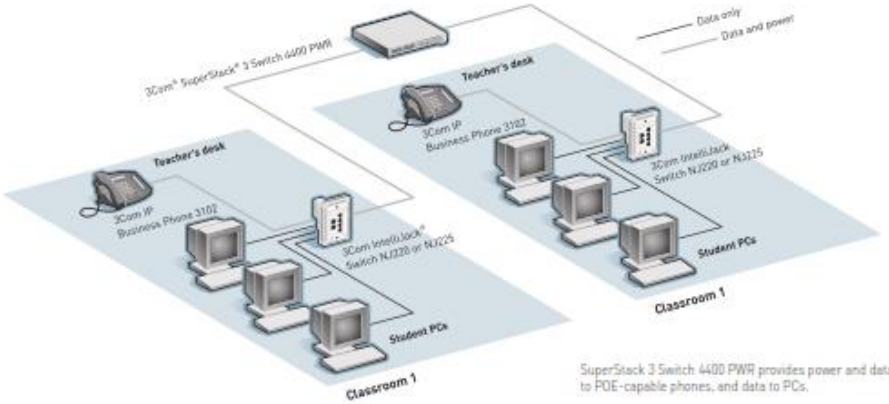
Network Health Check	An activity-auditing service focused on improving network performance and productivity Includes traffic monitoring, utilization analysis, problem identification, and asset deployment recommendations Extensive report provides blueprint for action
Network Design	Includes review of business plan, extensive inventory of requirements, and complete design document specifying implementation details
Network Installation	Experts set up and configure equipment and integrate technologies to maximize functionality and minimize business disruption Service may include physical site survey and network design and engineering based on evaluation of business objectives
Project Management	Provides extra focus and resources that special projects demand 3Com engineer(s) manage entire process from initial specifications to post-project review Using structured methodology, requirements are identified, projects planned, and progress of implementation activities tracked
3Com Guardian™ Maintenance Service	Provides comprehensive onsite support, including advance hardware replacement, telephone technical support, and software upgrades: • Telephone support backed by powerful call-tracking database and replication laboratory • Software upgrades ensure access to pertinent patches
3Com Express™ Maintenance Service	Benefits customers who prefer to maintain own hardware Bolsters in-house resources with convenient and speedy access to 3Com hardware replacements, software upgrades, and telephone support

For additional information, please visit www.3com.com/services

SUPERSTACK 3 SWITCH 4400s IN AN ENTERPRISE 10G NETWORK

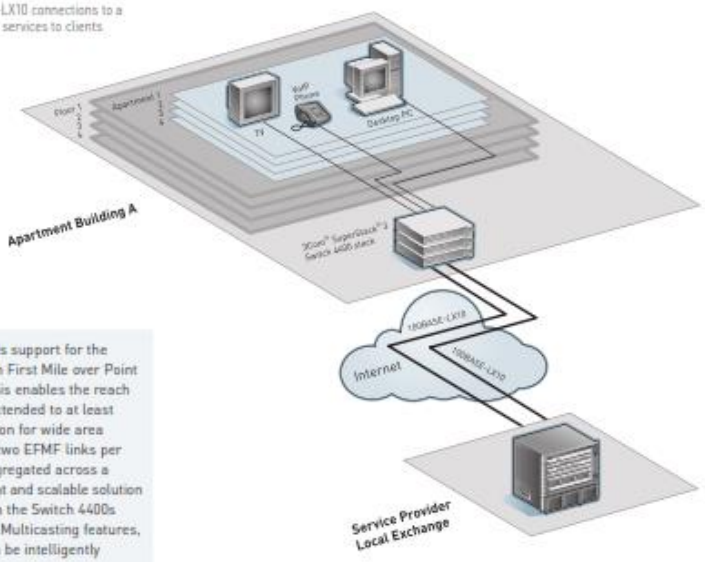


SUPERSTACK 3 SWITCH 4400 PWR AND POWER OVER ETHERNET



SuperStack 3 Switch 4400 PWR provides power and data to POE-capable phones, and data to PCs.

SuperStack 3 Switch 4400, with 100BASE-LX10 connections to a local service provider, provides converged services to clients within a 10km radius.



The SuperStack 3 Switch 4400 adds support for the emerging IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber (EFMF) standard. This enables the reach of Fast Ethernet over fiber to be extended to at least 10km, giving a cost effective solution for wide area Ethernet distribution. Support for two EFMF links per switch, or multiple EFMF links aggregated across a stack of switches, enables a resilient and scalable solution to be implemented. Combined with the Switch 4400s powerful QoS, Traffic Shaping and Multicasting features, the available uplink bandwidth can be intelligently shared between users.

SPECIFICATIONS

CONNECTORS
24 or 48 auto-negotiating 10BASE-T/100BASE-TX ports configured as Auto MDI/MDIX

24 auto-negotiating In-Line Power 10BASE-T /100BASE-TX ports configured as Auto MDI/MDIX (24-port PWR only)

2 module slots accommodating media modules or stacking modules

All fiber connectors are MT-RJ (LC connector on SuperStack 3 Switch 4400 100BASE-LX10 Module, 3C17229)

SECURITY
RADIUS (RFC 2865, RFC 2869)

Session accounting (RFC 2866)

SSH v2 (SSH Secure Shell, 'PuTTY', OpenSSH)

IEEE 802.1X network login

STACKING
Up to 384 10/100 front panel ports

Mix and match Switch 4400 24-port (3C17203), 4400 48-port (3C17204), and 4400 PWR (3C17205)*

PERFORMANCE
24-port

8.8 Gbps forwarding bandwidth

6.6 million packets per second

8,000 MAC addresses supported

48-port

13.6 Gbps forwarding bandwidth

10.1 million packets per second

8,000 MAC addresses supported

RELIABILITY
(MTBF @ 40°C)

24-port: 29 years (254,000 hours)

24-port PWR: 26 years (231,000 hours)

48-port: 20 years (179,000 hours)

DIMENSIONS
Height: 43.6 mm (1.7 in or 1U)

Width: 440 mm (17.3 in)

Depth:

24-port PWR: 304 mm (12.0 in)
all others: 274 mm (10.8 in)

Weight:

24-port: 2.8 kg (6.2 lb)
24-port PWR: 4.6 kg (10.1 lb)
48-port: 3.2 kg (7.1 lb)

ENVIRONMENTAL REQUIREMENTS
Operating temperature: 0° to 40°C (32° to 104°F)

Storage Temperature:
-40° to +70°C (-40° to +158°F)

Operating Humidity:
10% to 90% relative humidity noncondensing

Standards: EN60068 (IEC68)

INDUSTRY STANDARDS SUPPORTED
IEEE 802.1D (STP)

IEEE 802.1p (CoS)

IEEE 802.1Q (VLANs)

IEEE 802.1w (RSTP)

IEEE 802.1X (Security)

IEEE 802.3ab (1000BASE-T)

IEEE 802.3ad (Link Aggregation)

IEEE 802.3af (Power over Ethernet)

IEEE 802.3ah (Ethernet in First Mile over Point to Point Fiber - EFMP)

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

IEEE 802.3x (Flow Control)

IEEE 802.3z (Gigabit Ethernet)

SAFETY AGENCY CERTIFICATIONS
24-port: UL1950, EN60950, CSA22.2 No. 950, IEC 60950

24-port PWR, and 48-port: UL60950, EN60950, CSA2.2 No. 60950, IEC 60950

EMISSIONS
EN55022 Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A, AS/NZS 3548 Class A, CNS 13438 Class A

CISPR 22 CLASS A, EN61000-3-2, EN61000-3-3 (24-port PWR only)

Immunity: EN55024

Heat Dissipation:

24-port: 100 W maximum (341 BTU/hr maximum)

24-port PWR: 275 W maximum (938 BTU/hr maximum)

48-port: 120 W maximum (410 BTU/hr maximum)

POWER SUPPLY
AC Line Frequency 50/60 Hz

Input Voltage 90-240 VAC

Current Rating:

24-port: 2.5A maximum

48-port: 2.8A maximum

SNMP STANDARDS
SNMP Protocol (RFC 1157)

MIB-II (RFC 1213)

Bridge MIB (RFC 1493)

RMON MIB II (RFC 2021)

Remote Monitoring MIB (RFC 1757)

Interface MIB (RFC 2233)

Remote Poll MIB (RFC 2925)

MAU MIB (RFC 2668)

SNTP (RFC 2030)

PoE MIB (RFC 484) (24-port PWR only)

MANAGEMENT
Web interface

Command line interface

SNMP compatibility

Management through 3Com management applications

- 3Com Network Supervisor
- 3Com Network Director
- 3Com Network Administrator
- 3Com Enterprise Management Suite

WARRANTY
Limited Lifetime Hardware Warranty. Limited Software Warranty for ninety (90) days. See www.3com.com/warranty for details.

OTHER BENEFITS
Other Service Benefits: Advance hardware replacement with same day shipment for North America and Western Europe. Next day shipment for rest of world. Calls must be received by published cut-off times. 90 days of telephone technical support. Limited software updates. See www.3com.com/warranty for more detail.

Register products at http://eSupport.3com.com.

SERVICE
Americas:
www.3com.com/products/en_US/global_services

International:
http://emea.3com.com/globalservices

* Stacking compatibility also for previously sold Switch 4400 FX model (3C17210). With the purchase of new Switch 4400s on or after May 1, 2006 and subsequent product registration, includes right and license to upgrade Switch 4400 SE model units (3C17206) for compatible stacking.

ORDERING INFORMATION

PRODUCT DESCRIPTION	3COM SKU
3Com SuperStack 3 Switch 4400 24-port	3C17203
3Com SuperStack 3 Switch 4400 48-port	3C17204
3Com SuperStack 3 Switch 4400 PWR	3C17205
Optional Modules and Accessories	
3Com SuperStack 3 Switch 4400 1000BASE-T Module	3C17220
3Com SuperStack 3 Switch 4400 1000BASE-SX Module	3C17221
3Com SuperStack 3 Switch 4400 100BASE-FX Module	3C17222
3Com SuperStack 3 Switch 4400 1000BASE-LX Module	3C17223
3Com SuperStack 3 Switch 4400 100BASE-LX10 Module*	3C17229
3Com SuperStack 3 Switch 4400 Stacking Kit *(Two stacking modules and cable to stack two Switch 4400s)*	3C17227
3Com SuperStack 3 Switch 4400 Stack Extender Kit *(One stacking module, one cascade module and one cable for adding more Switch 4400s to an existing Switch 4400 stack)*	3C17228

Express™ Service Plans†	Americas	EMEA / AP‡
3Com SuperStack 3 Switch 4400 24-port	3CS-EXP-05E	3CS-EXP-X305
3Com SuperStack 3 Switch 4400 48-port	3CS-EXP-08E	3CS-EXP-X309
3Com SuperStack 3 Switch 4400 PWR	3CS-EXP-06E	3CS-EXP-X307

* Switch 4400 software version 3.1, minimum, required for operation.

† Includes telephone support, advance hardware replacement, and software upgrades.

‡ Europe, Middle East, Africa and Asia Pacific

Visit www.3com.com for more information about 3Com secure converged network solutions.

3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064
3Com is publicly traded on NASDAQ under the symbol COMS.

400679-017 05/06

ANEXO 3

IBM Systems and Technology Group
Hoja de especificaciones

System x

IBM System x3650 M3

Servidor de rendimiento optimizado para aplicaciones de vital importancia

IBM

Características destacadas:

- Aumente la rentabilidad con mayor rendimiento por watt
- Simplifique la gestión y el mantenimiento gracias a un diseño flexible
- Gestione los riesgos mediante arquitecturas resistentes y entornos virtualizados.

Repleto de innovación

El IBM System x3650 M3 ofrece un rendimiento extraordinario para sus aplicaciones más importantes. Su diseño para un uso eficiente de la energía admite más cores, memoria y capacidad de disco en un paquete 2U ampliable que es fácil de mantener y gestionar. Con más potencia informática por watt y los últimos procesadores Intel ® Xeon®, podrá reducir costos mientras que mantiene la velocidad y la disponibilidad.

Simplifique la gestión y el mantenimiento

El x3650 M3 ofrece un diseño flexible y ampliable y una ruta de actualización sencilla a 16 unidades de disco duro (HDD) o unidades de estado sólido (SSD) y 192 GB de memoria. Sus herramientas de gestión de sistemas, tales como el diagnóstico avanzado, un brazo de gestión de cableado y la capacidad de controlar los recursos desde un único punto, hacen que sea un sistema fácil de implementar, integrar, mantener y gestionar.

Reduzca los riesgos y mantenga la disponibilidad

Gracias a los nuevos adaptadores integrados Redundant Array of Independent Disks (RAID) a 6 Gigabits por segundo (Gbps) y el doble de rendimiento de entrada/salida (E/S), el x3650 M3 ofrece una arquitectura robusta ideal para aplicaciones de vital importancia y para entornos de virtualización. El soporte de memoria avanzada y la mayor capacidad de disco le permiten hacer uso de mayores velocidades de procesamiento sin sacrificar tiempo de actividad.

Algunas configuraciones de x3650 M3 forman parte de IBM Express Advantage Portfolio, diseñado para atender las necesidades de las empresas de tamaño medio. Fáciles de gestionar, los modelos y las configuraciones Express varían según el país.

Para más información

Página principal de System x en México: http://www.ibm.com/mx/systems/x
Vea las promociones de System x en México:
http://www.ibm.com/systems/promocionesystemx
Encuentre su Business Partner más cercano en México:
http://www-304.ibm.com/partnerworld/wps/bplocator/search.jsp

Resumen de características de IBM System x3650 M3

Formato y altura	Rack/2U
Procesador (máx.)	Hasta dos procesadores Intel Xeon de la serie 5600 a 3.46 GHz de seis cores (3.60 GHz en la versión de cuatro cores) con tecnología QuickPath Interconnect (QPI)
Número de procesadores (est./máx.)	Uno/dos
Memoria caché (máx.)	Hasta 12 MB de nivel 3 (L3)
Memoria (máx.)	Módulos RDIMM (Registered Dual Inline Memory Module) DDR-3 (Double Data Rate 3) de 192 GB a través de 18 ranuras Dual Inline Memory Module (DIMM) o UDIMM (Unregistered DIMM) DDR-3 de 48 GB a través de 12 ranuras DIMM
Ranuras de expansión	Cuatro
Bahías de disco (total/hot-swap)	Hasta dieciséis unidades de disco duro (HDD) de 2,5" hot-swap Serial Attached SCSI (SAS)/Serial Advanced Technology Attachment (SATA) o Unidades de estado sólido (SSD) como máximo
Almacenamiento interno máximo	Hasta 16,0 TB [1] (SAS/SATA hot-swap)
Interfaz de red	Dos puertos integrados, además de dos puertos opcionales Gigabit Ethernet (GbE)
Fuente de alimentación (est./máx.)	Una/dos; 460 W CA, 675 W CA, 675 W CA de alta eficiencia o 675 W CC (depende del modelo)
Componentes hot-swap	Fuentes de alimentación, módulos de ventilación, discos
Compatibilidad con RAID	RAID-0, -1, -10 a 6 Gbps o RAID-0, -1, -10, -5, -50 a 6 Gbps con caché de 256 MB o 512 MB y respaldo por batería opcional adicional, según el modelo
Certificado para el Sistema de construcción de equipos de redes (Network Equipment Building System o NEBS) **1/Instituto Europeo de Normas de Telecomunicaciones** (European Telecommunication Standards Institute o ETSI)	Cumplimiento equivalente para la fuente de alimentación de CA y CC (depende del modelo)
Cumplimiento de eficiencia energética	Cumple con las normas de eficiencia energética 80-PLUS y ENERGY STAR (depende del modelo)
Gestión de sistemas	IBM Integrated Management Module (IMM) con Virtual Media Key para la activación de presencia remota opcional, Predictive Failure Analysis, diodos emisores de luz (LED) de diagnóstico, panel Light Path Diagnostics, Automatic Server Restart, IBM Systems Director e IBM Systems Director Active Energy Manager
Sistemas operativos compatibles	Microsoft® Windows® Server2008 R2 y 2008, Red Hat Enterprise Linux® (RHEL), SUSE Linux Enterprise Server (SLES), VMware ESX y ESXi, Oracle Solaris 10 (depende del modelo)
Garantía limitada	Garantía de tres años de unidad sustituible por el cliente (CRU) e in situ limitada

IBM de México, S. de R.L.
Alfonso Nápoles Gándara 3111,
Peña Blanca
01210 México, D.F.
México

El sitio web de IBM está disponible en:
http://www.ibm.com/mx/es

[1] Disponible en el segundo trimestre de 2011.

MX-OCT11-3650M3

ANEXO 4

IBM System Storage DS3500 Express

Affordable performance and flexibility with greater scalability, efficiency and ease of use

Highlights

- Deliver mid-range performance and scalability at entry-level prices with 6 Gbps SAS systems
- Leverage built-in management expertise in intuitive and powerful storage management software
- Deliver simplified data protection management and automated recovery with Dynamic Disk Pooling
- Support Enhanced Global Mirroring over IP and/or Fibre Channel
- Deliver continuous data security with full disk encryption and support high-performing solid-state drives (SSDs)
- Comply with Network Equipment Building System (NEBS) and European Telecommunication Standards Institute (ETSI) and support 48 V DC power supplies

IBM® System Storage® DS3500 Express® combines best-of-breed development with leading 6 Gbps host interface and drive technology. With its simple, efficient and flexible approach to storage, the DS3500 Express is a cost-effective, fully integrated complement to IBM System x® servers, IBM BladeCenter® and IBM Power Systems™. By offering substantial improvements at a price that fits most budgets, the DS3500 Express delivers superior price/performance ratios, functionality, scalability and ease of use for the entry-level storage user.

The DS3500 Express offers:

- Scalability to mid-range performance and features starting at entry-level prices
- Efficiency to help reduce annual energy expenditures and environmental footprints
- Simplicity that does not sacrifice control with the perfect combination of robustness and ease of use

Delivers mid-range performance and scalability

Building on the solid foundation of 3 Gbps SAS technology, 6 Gbps SAS is the enterprise version of SAS. This 6 Gbps SAS offers increased performance, scalability and reliability enhancements to support the ever-increasing reliance on information, while delivering the outstanding value that organizations demand.

Delivering solid input and output per second (IOPS) and throughput, the DS3500 Express controllers offer balanced and sustainable performance. With up to 4,000 megabytes (MB) per second and 40,000 IOPS in sustained drive reads, the DS3500 Express is equally adept at delivering throughput to bandwidth-intensive applications and IOPS to databases and Microsoft Exchange.

The DS3500 Express has enhanced scalability of up to 576 terabytes (TB) when fully expanded up to 192 drives. By dynamically adding drive enclosures (up to 15 EXP3512, 7 EXP3524 expansion enclosures or a mix of the two) with virtually no downtime, you can quickly and seamlessly respond to growing capacity demands. This scalability also improves overall system performance by distributing the server's I/O requests across a greater number of drives.

Provides intuitive storage management without sacrificing control

IBM System Storage DS Storage Manager software has combined robustness with ease-of-use—two attributes not commonly found together in entry to mid-range storage systems. The graphical user interface used by DS Storage Manager is ideally suited for full-time storage administrators who want complete control over their storage configurations as well as part-time system administrators who need an intuitive interface that helps them ensure optimal storage utilization. And with its industry-unique dynamic capabilities, administrators can support on-the-fly reconfigurations without interrupting storage system input/output (I/O). New Dynamic Disk Pooling (DDP) technology dramatically simplifies data-protection setup and can virtually eliminate the need for unscheduled drive maintenance. DDP is a self-healing data-protection technology that negates the need for complex RAID calculations, fully utilizes all of the disk drives in the array and delivers consistent system performance.

In addition to DDP, DS Storage Manager has fully integrated features that allow administrators to choose the method that best meets their data utilization and protection requirements:

- IBM Enhanced FlashCopy® creates near-instantaneous, capacity-efficient, point-in-time volume images that provide logical volume for uses such as file restoration and backup
- Volume Copy creates a complete physical copy—or clone—of a volume within a storage system; this unique entity can be assigned to any host and used for application testing or development, information analysis or data mining
- Thin provisioning with DDP helps to create the appearance of more disk space than is actually available, which helps to consume less space; it also offers the flexibility to increase space as data grows

Optional premium features deliver enhanced capabilities for the DS3500 Express system.

- **Disaster Recovery option**—Provides 16 Enhanced Remote Mirrors and 32 Enhanced Global Mirrors; also offers multiple options for disaster-recovery deployment and supports replication over Fibre Channel or IP for the DS3500 system

- **Backup and Restore option**—Allows 512 Enhanced FlashCopy images on the DS3500 system; Enhanced FlashCopy technology delivers easier setup of shared versus dedicated repositories and reduces capacity requirements and copy-on-write capacity consumption
- **Performance Read Cache option**—Utilizes SSDs as a level-two data cache, significantly improving read performance from spinning media; Performance Read Cache is extremely easy to set up and, once implemented, it automatically identifies the data that is read most frequently and copies it into cache for fast access
- **Super Key option**—Combines all of the features into one single key for easy deployment and management

Supports VMware and heterogeneous operating systems

The DCS3500 Express offers the scalability, availability and integration necessary to power VMware implementations of all sizes. Its heterogeneous operating system support provides flexibility to manage a wide range of storage needs. It also includes support for VMware vSphere application programming interface (API) for Array Integration. And two application-aware plug-ins enable vCenter and Storage Replication Adapter (SRA) for efficient management.

Enables energy-saving implementations

With rising energy expenses and IT space constraints, efforts to reduce power consumption in a small IT footprint have quickly come to the forefront as hot-button IT issues for many organizations. To respond to these challenges, IBM has made great strides in energy-efficient implementations with the DS3500 Express, which introduces power-saving features designed to have virtually no impact on performance, scalability or functionality.

Smaller form-factor 2.5-inch SAS drives, one of multiple drives supported by the DS3500 Express, provide up to three times more IOPS per watt in power consumption than 3.5-inch

drives and enable twice as many drives to reside in the same 2U of rack space. These drives also deliver impressive IOPS performance in a small form factor with minimal impact on power consumption or heat dissipation.

Energy-efficient power supplies help ensure just that—energy efficiency. By efficiently converting AC power from electric utilities into DC power used by the storage system, the DS3500 Express power supplies ensure that overall annual expenditures are lower than other, less-efficient implementations. And with low heat dissipation, the DS3500 Express serves a key role in an overall energy-saving and green solution.

With a DC-powered model for 24-drive enclosures with NEBS and ETSI compliance, the DS3500 Express offers savings in energy expenses, meets standard telecommunications requirements and minimizes risk in harsh environments.

The DS3500 Express continues the tradition of superior disk use that enables users to achieve maximum return on investment (ROI) on their storage investments. The DS series can deliver up to two times the disk use of leading competitors, enabling organizations to achieve maximum performance with fewer drives and less energy consumption.

Enables IBM DB2 Administration Server and SAN tiering

Administrators can now benefit from tiered IBM DB2® Administration Server and storage area network (SAN) implementations with multiprotocol host connectivity. The DS3500 Express supports intermixing four 1 Gbps iSCSI, two 10 Gbps iSCSI—dual-ported—or four 8 Gbps Fibre Channel host ports with its native 6 Gbps SAS interfaces. This flexible and multipurpose dual-protocol approach enables organizations to implement a single storage system to support all of their shared storage requirements and helps improve productivity, reliability and cost savings. These implementations offer additional benefits, as well:

- Low-cost, high-speed SAS delivers the best value and performance for direct-attached storage implementations.
- Data centers with existing IP networks or Fibre Channel SAN infrastructures can cost-effectively implement these additional host interfaces as required; 1 Gbps iSCSI is ideal for low-cost implementations for secondary servers, and Fibre Channel is well positioned for high-performance and robust deployments.
- Future-proof storage provides seamless integration to an existing 1 Gbps iSCSI infrastructure and is ready for the inevitable move to 10 Gbps iSCSI.

Offers continuous data security

In the lifecycle of a hard drive, it will, at some point, be out of the user's control either through theft, offsite service, repair or disposal. The DS3500 Express combines local key management and drive-level encryption for comprehensive data security designed to protect data throughout the life of the drive without sacrificing storage system performance or ease of use.

Full disk encryption (FDE) provides data security at the most basic level—the hard drive. FDE protects against many exposures and vulnerabilities all at once. This drive-level encryption helps ensure data security in the event of a drive loss, theft or retirement. The FDE engine performs encryption without a performance penalty, which gives you the highest levels of data security while retaining optimal performance.

Fully integrated into the DS Storage Manager as a premium feature upgrade, local key management provides the necessary management and protection of self-encrypting disk (SED) drives by using a single authorization scheme, or lock key, which can be set and applied to all SED drives in the DS3500 Express. The DS Storage Manager maintains and controls the key linkage and communications with the SED drives, secures user-selected logical drive groups and initiates the instant secure erase feature for users desiring even more peace of mind when servicing, decommissioning or repurposing drives. With local encryption services, FDE key management is transparent to day-to-day storage administration, making SED drives as easy to manage as traditional drives.

Enables uptime all the time

The DS3500 Express ensures continuous access to data. It carries on the IBM legacy of high-availability system design with redundant components, automated path failover and extensive online administration capabilities that maximize computational efficiency and productivity, ensuring there is virtually no single point of failure. This design helps keep these environments universally productive. New DDP technology is standard on the DS3500 Express and virtually eliminates maintenance worries by self tuning, rebalancing data and maintaining consistent performance even during drive failures.

Supports capacity needs with tiered storage

The DS3500 Express can cost-effectively support an organization's complete range of data capacity requirements—from nearline static data to highly used applications—through support for mixed drive types in a single storage system. The DS3500 Express accomplishes this with support for high-performance SAS drives, nearline SAS drives, SSDs and SED drives. Nearline SAS drives are also the clear replacement of SATA drives. Competitively priced to SATA drives, nearline SAS drives significantly outperform SATA and do so with greater reliability.

Now you can address even more granular and specific requirements for your application needs, whether they include security for data at rest, leading performance or energy efficiency. This exciting capability maximizes storage density and provides a more efficient use of enclosures when implementing a tiered storage solution.

Centralizes storage device management

IBM Tivoli® Storage Productivity Center for Disk Select V4.2.2 is designed to provide storage device configuration, performance monitoring and management of SAN-attached devices from a single console. In addition, it includes performance-monitoring capabilities for the DS3500 Express.

Tivoli Storage Productivity Center for Disk Select V4.2.2 provides the following features:

- Continuous real-time monitoring and fault identification to improve SAN availability
- Performance reporting across multiple arrays from a single console
- Monitoring of metrics such as throughput, I/O, data rates and cache use
- Reception of timely alerts that can enable event action based on policies when thresholds are exceeded
- Improved storage ROI by helping to keep SANs up and running
- Reduced storage administration costs by simplifying the management of complex SANs

Handles key applications and workloads

The DS3500 Express offers these additional capabilities:

- Consolidation and virtualization: Balanced performance, low-cost consolidation and unparalleled configuration flexibility make the DS3500 Express ideally suited for smaller consolidation and virtualization implementations in which an individual storage system supports diverse workloads and application requirements.
- Departmental and remote sites: The DS3500 Express offers the right amount of performance, simplicity and functionality that a part-time administrator can use at a price that won't break an organization's budget, allowing multiple sites to be self-sufficient.
- Transactional workloads: Efficient IOPS make the DS3500 Express well suited for transactional workloads—including online transaction processing, databases and email—that are the core of every organization's critical applications.
- Data warehousing: Solid throughput, 6 Gbps SAS, 8 Gbps Fibre Channel and 10 Gbps iSCSI interfaces make the DS3500 Express well suited for data-warehousing environments in which an individual storage system must process large amounts of data.
- Business-critical applications: With bullet-proof reliability, support for SED drives and exceptional uptime, the DS3500 Express supports business-critical applications where data must be protected and available when needed.
- Secondary storage: Support for redundant array of independent disks (RAID) 6, DDP and native language SAS drives means the DS3500 Express can store large amounts of data cost effectively, with confidence that it is fully protected.
- Clustered topologies: SAS-based shared storage and Fibre Channel or iSCSI SAN implementations are ideal for clustering solutions such as Microsoft Cluster Server and Oracle Real Application Clusters when transitioning from a direct-attached storage implementation.
- Streaming video: Large-block I/O applications, such as world-class broadcasting, rich-media storage networks, content creation, modeling and publishing benefit from the additional bandwidth that the DS3500 Express series offers.
- Data mining: With Fibre Channel and SAS host connectivity, organizations can accelerate and scale simulation, visualization, modeling and rendering applications easily to accelerate large dataset I/O rates, as well as cost-effectively scale and share information across the organization for high-level collaboration.

- Backup and restore: With the ability to mirror data between storage systems over IP and/or Fibre Channel host ports, the DS3500 Express can support short backup windows and recovery times for high productivity.
- Storage solution: The DS3500 Express offers enhanced Tivoli Storage FlashCopy services, thin provisioning and advanced software features for small and mid-size businesses.
- Data protection: The DS3500 Express offers simplified provisioning, improved rebuild times and more consistent performance under failure via selectable disk pooling.
- Campus area replication: When replicating data across a high-speed Fibre Channel SAN or IP networks, data can be mirrored synchronously, ensuring that remote sites have the exact same data as the local site at all times.

IBM System Storage DS3500 Express at a glance

Characteristics	
Part number	1746A2S DS3512 Express Single Controller Storage System 1746A2D DS3512 Express Dual Controller Storage System 1746A4S DS3524 Express Single Controller Storage System 1746A4D DS3524 Express Dual Controller Storage System 1746T4D DS3524 Express DC Dual Controller Storage System
RAID controller	Single or dual active, hot-swappable controllers
Cache	1 gigabyte (GB) cache per controller with 2 GB upgrade (battery-backed)
Host interface	Four options: • Four or eight 6 Gbps SAS ports • Eight 8 Gbps Fibre Channel ports and four 6 Gbps SAS ports • Eight 1 Gbps iSCSI ports and four 6 Gbps SAS ports • Four 10 Gbps iSCSI ports and four 6 Gbps SAS ports
Drive interface	Single controller subsystem: One 6 Gb SAS drive port Dual controller subsystem: Two 6 Gb SAS drive ports
Supported drives	**6 Gbps SAS 3.5-inch drives:** • 300 GB 15k rpm • 450 GB 15k rpm • 600 GB 15k rpm • 2 TB 7.2k rpm nearline • 3 TB 7.2k rpm nearline • 600 GB 15k rpm SED **6 Gbps SAS 2.5-inch drives:** • 300 GB 10k rpm • 600 GB 10k rpm • 900 GB 10k rpm • 500 GB 7.2k rpm nearline • 300 GB 10k rpm SED • 1 TB 7.2k rpm nearline **Solid-state SAS 2.5-inch drives:*** • 200 GB SSD • 400 GB SSD

IBM System Storage DS3500 Express at a glance			
Data protection levels	RAID levels 0, 1, 3, 5, 6, 10 and/or DDP		
Software features	Thin provisioning with DDP, 128 storage partitions, 32 Enhanced FlashCopy images, host-attachment support for Microsoft Windows and Linux on Intel with firmware 7.84 and higher		
Maximum drives supported	• Up to 192 drives—high-performance SAS drives, nearline SAS drives, SSDs and SED SAS drives • EXP3512 (2U 12 3.5-inch drives) and EXP3524 (2U 24 2.5-inch drives) enclosures, which can be intermixed behind a DS3500 Express enclosure		
Fans and power supplies	Dual redundant, hot-swappable		
Rack support	2U, 19-inch, industry-standard rack		
Management software	IBM System Storage DS Storage Manager		
SAN support	Supported Fibre Channel switches and directors, and IP switches		
Warranty	Three-year parts and labor warranty, 9x5 next business day, upgradable to 24x7 with four-hour response		
Physical characteristics			
Dimensions (H x W x D)	DS3512: 86.16 mm x 482.47 mm x 551.60 mm (3.39 in. x 18.99 in. x 21.72 in.) DS3524: 88.07 mm x 482.10 mm x 497.93 mm (3.47 in. x 18.98 in. x 19.60 in.)		
Supported systems	For a list of currently supported servers, operating systems, host bus adapters, clustering applications and SAN switches and directors, refer to the DS3500 Express Interoperability Matrix.		
Model	Model description	Interface	Model includes
1746-E2A/EXP3512 1746-E4A/EXP3524	Drive enclosure	6 Gb SAS	External security manager-embedded
Relative humidity (no condensation)	EXP3512/EXP3524 drive enclosure		
Operating range	20% – 80%		
Storage range	10% – 90%		
Maximum dew point	26°C (79°F)		
Maximum gradient	10% per hour		
Altitude ranges			
Operating	30.5 m below sea level to 3,048 m above sea level (100 ft below to 10,000 ft above)		
Storage	30.5 m below sea level to 3,048 m above sea level (100 ft below to 10,000 ft above)		
Transit	30.5 m below sea level to 12,000 m above sea level (100 ft below to 40,000 ft above)		
The tabulated power and heat dissipation values are the maximum measured operating power.			
Acoustic noise	EXP3512/EXP3524 drive enclosure		
Sound power	6.5 bel		
Sound pressure	65 dBA		
Power input	EXP3512/EXP3524 drive enclosure		
Nominal voltage range	90 – 264 V ac		
Frequency range	50 – 60 Hz		
Maximum operating current	3.90 A at 115 V ac 2.06 A at 230 V ac		

For more information

To learn more about the IBM System Storage DS3500 Express, please contact your IBM representative or IBM Business Partner, or visit ibm.com/systems/storage/disk/ds3500

For a list of currently supported servers, operating systems, host bus adapters, clustering applications and SAN switches and directors, refer to the DS3500 Express Interoperability Matrix available at ibm.com/systems/support/storage/config/ssic

For availability dates, configuration options and attachment capabilities, refer to ibm.com/systems/storage/disk

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: ibm.com/financing

IBM Corporation
Systems and Technology Group
Route 100
Somers, NY 10589

Produced in the United States of America
February 2013

Actual available storage capacity may be reported for both uncompressed and compressed data and will vary and may be less than stated.

* Limitation: Maximum of 24 SSDs per system (a system is defined as the DS3500 Express storage controller and all attached EXP3524 expansion units)

Please Recycle

TSD03097-USEN-11

ANEXO 5

Executive Overview

InsightVM_Ejecutivo

Audited on August 30, 2017

Reported on September 5, 2017

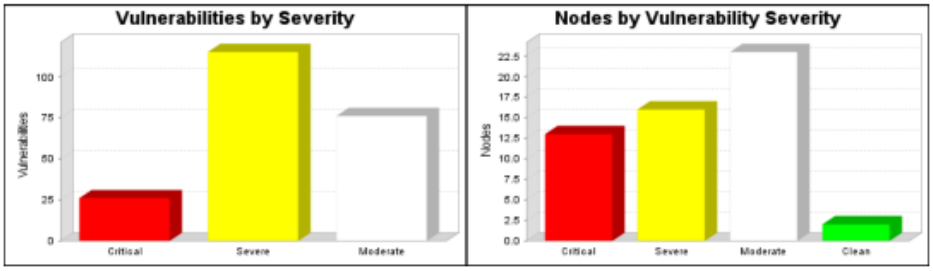
1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

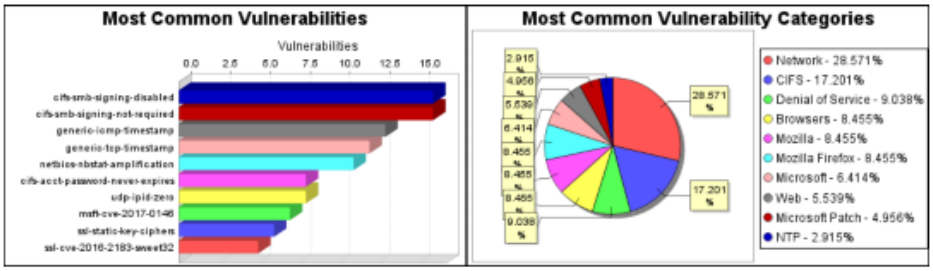
Site Name	Start Time	End Time	Total Time	Status
Gobernacion	August 30, 2017 23:31, COT	August 31, 2017 09:21, COT	9 hours 49 minutes	Success

There is not enough historical data to display overall asset trend.

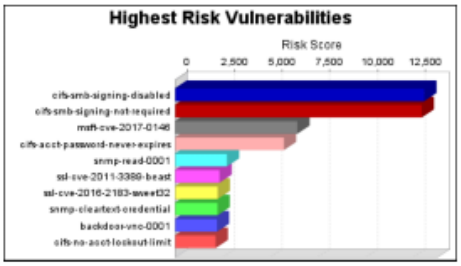
The audit was performed on 25 systems, 25 of which were found to be active and were scanned.



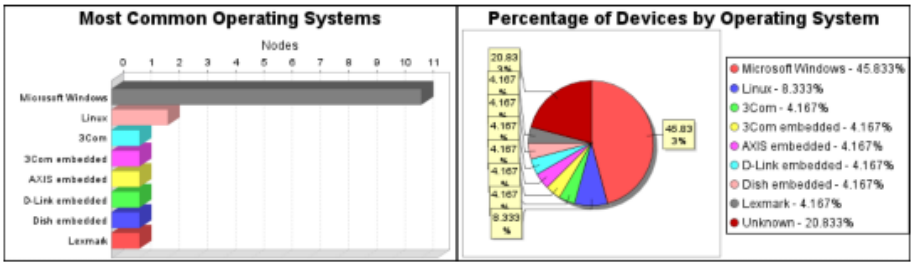
There were 217 vulnerabilities found during this scan. Of these, 26 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 115 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 76 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 13 of the systems, making them most susceptible to attack. 16 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 23 systems. No vulnerabilities were found on the remaining 2 systems.



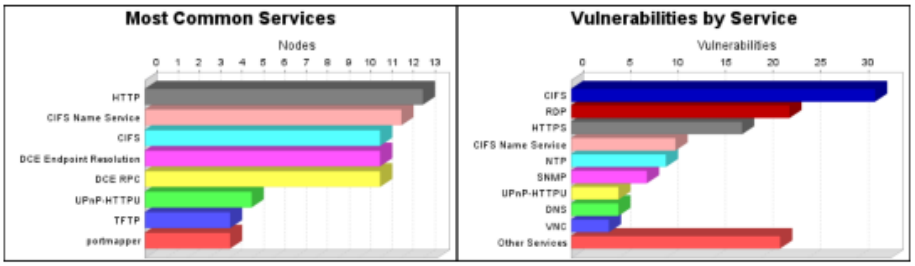
There were 16 occurrences of the cifs-smb-signing-disabled and cifs-smb-signing-not-required vulnerabilities, making them the most common vulnerabilities. There were 98 vulnerability instances in the Network category, making it the most common vulnerability category.



The cifs-smb-signing-disabled vulnerability poses the highest risk to the organization with a risk score of 13,090. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
There were 10 operating systems identified during this scan.



The Microsoft Windows operating system was found on 11 systems, making it the most common operating system.
There were 43 services found to be running during this scan.



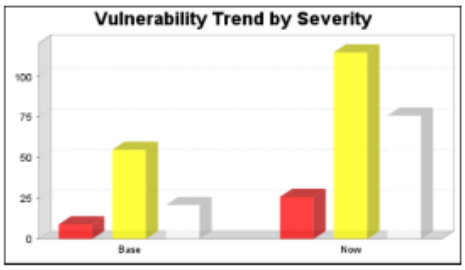
The HTTP service was found on 13 systems, making it the most common service. The CIFS service was found to have the most vulnerabilities during this scan with 32 vulnerabilities.

2. Trend Analysis

5 new nodes were discovered, but one previously previously discovered node was not found. This reduces the number of actives nodes to 25.

The overall number of vulnerabilities rose from 85 to 217. The number of critical vulnerabilities increased from 9 to 26. The number of severe vulnerabilities increased from 55 to 115. The number of moderate vulnerabilities increased from 21 to 76.

The network is now at greater risk of compromise. It is important to address reported vulnerabilities as quickly as possible. Failure to do so greatly increases the risk of compromise.



The overall number of services rose from 148 to 218. The newly discovered services were responsible for 65 vulnerabilities. Whenever adding new hardware or software, it is critical to apply all available patches. The configuration of the service should also be checked to make sure all possible security measures are in place.

ANEXO 6

Highest Risk Vulnerabilities

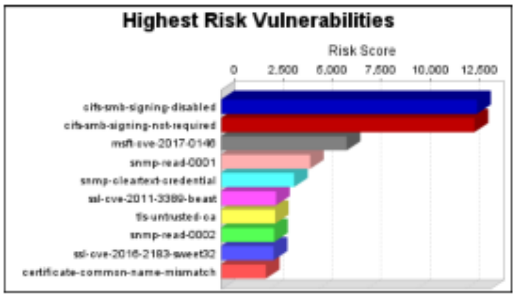
InsightVM_MayorRiesgoVulnerabilidades

Audited on August 30, 2017

Reported on September 5, 2017

Table of Contents

1. Executive Overview



The cifs-smb-signing-disabled vulnerability poses the highest risk to the organization with a risk score of 13,090. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

2. Highest Risk Vulnerability Details

2.1. SMB signing disabled (cifs-smb-signing-disabled)

Category	CIFS
CVSS score	7.3 (AV:A/AC:M/Au:N/C:C/I:C/A:N)
Risk Score	13,090
References	URL: http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

2.2. SMB signing not required (cifs-smb-signing-not-required)

Category	CIFS
CVSS score	6.2 (AV:A/AC:H/Au:N/C:C/I:C/A:N)
Risk Score	12,963
References	URL: http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

2.3. Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability (msft-cve-2017-0146)

Category	Microsoft, Microsoft Patch
CVSS score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Risk Score	6,431
References	CVE-2017-0146, MSKB: 4012212, MSKB: 4012213, MSKB: 4012214, MSKB: 4012598, MSKB: 4012606, MSKB: 4013198, MSKB: 4013429, MS17-010

2.4. Default or Guessable SNMP community names: public (snmp-read-0001)

Category	SNMP
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	4,568
References	BID: 2896, BID: 3795, BID: 3797, CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-2001-0514, CVE-2002-0109, CVE-2010-1574, XF: 6576, XF: 7827

2.5. SNMP credentials transmitted in cleartext (snmp-cleartext-credential)

Category	Remote Execution, SNMP
CVSS score	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Risk Score	3,742
References	CERT: CA-2002-03

2.6. TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)

Category	Network
CVSS score	4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
Risk Score	2,817
References	CVE-2011-3389, URL: http://vnhacker.blogspot.co.uk/2011/09/beast.html

2.7. Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)

Category	Network
CVSS score	5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
Risk Score	2,776
References	URL: http://httpd.apache.org/docs/2.2/mod/mod_ssl.html, URL: http://nginx.org/en/docs/http/configuring_https_servers.html, URL: https://support.microsoft.com/en-us/kb/954755

2.8. Default or Guessable SNMP community names: private (snmp-read-0002)

Category	SNMP
CVSS score	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Risk Score	2,728
References	BID: 973, CVE-1999-0516, CVE-1999-0517, CVE-2000-0147, CVE-2010-1574, URL: ftp://ftp.sco.com/SSE/security_bulletins/SB-00.04a, URL: http://archives.neohapsis.com/archives/bugtraq/2000-02/0045.html

2.9. TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)

Category	Network, Rapid7 Critical
CVSS score	5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Risk Score	2,698
References	CVE-2016-2183, URL: https://sweet32.info/, URL: https://www.openssl.org/blog/blog/2016/08/24/sweet32, URL: https://access.redhat.com/articles/2548661

2.10. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Category	HTTP, Web
CVSS score	7.1 (AV:N/AC:H/Au:N/C:C/I:C/A:N)

Highest Risk Vulnerabilities

Risk Score	2,305

ANEXO 7

Risk Scorecard

September 5, 2017 11:27:45 COT

InsightVM_PuntajeRiesgo

Site: Gobernacion

C

Your site's grade of C is based on its average asset risk score of 10,427, is within 5% of the average 10,427 across all sites. Grades range from A (average risk per asset is more than 15% lower than the average across all sites) to F (average risk per asset is more than 15% higher than the average across all sites). Use the following scan data to determine the factors that affect risk the most.

Statistics

Assets: 34

Vulnerabilities: 935

Average vulnerabilities per asset: 27.5

Average asset risk score: 10,427

Last Scan

Asset(s) scanned: 25

Percentage of site scanned: 73.5%

Vulnerabilities

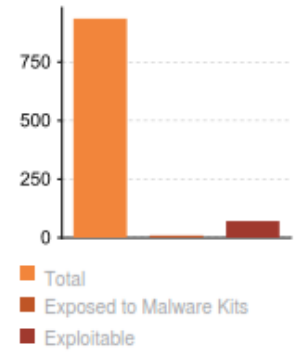
Vulnerabilities with known exploits: 7.6%

Exploits available for vulnerabilities: 90

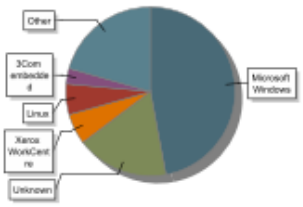
Vulnerabilities with known malware kits: 1.0%

Malware kits available for vulnerabilities: 1

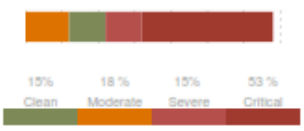
Vulnerabilities



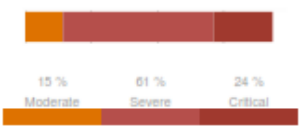
Assets by Operating System



Assets by Vulnerability Severity



Vulnerabilities by Severity



Top 10 Assets by Risk Score

IP Address	Host Name	Risk Score		
192.168.2.6	NO-TE-AGUANTO	252968	57	0
192.168.2.4	Servidor.GoberGuayas.local	16244	6	0
192.168.2.40	HP_Despacho	15696	2	0
192.168.2.50	ET0021B7F0108B	11003	3	0
192.168.2.56	DIGITAL	7912	14	1
192.168.2.1	null	5374	1	0
192.168.2.3	null	4285	11	0
192.168.2.63	UA001	3979	7	1
192.168.2.23	NERO-DELL	3561	0	0
192.168.2.148	DESKTOP-J3DL0JD	3262	7	1

ANEXO 8

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name: GOBERGUAYAS\SERVIDOR
IP address: 192.168.2.4
Security report name: GOBERGUAYAS - SERVIDOR (30-08-2017 18-55)
Scan date: 30/08/2017 18:55
Catalog synchronization date:
Security update catalog: Microsoft Update

Security Updates

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	3 security updates are missing.

Security Updates

Score	ID	Description	Maximum Severity
Missing	MS09-062	Security Update for Microsoft Visual Studio 2008 Service Pack 1 (KB972222)	Low
Missing	MS12-021	Security Update for Microsoft Visual Studio 2008 Service Pack 1 (KB2669970)	Important
Missing	MS11-049	Security Update for Microsoft Visual Studio 2008 Service Pack 1 XML Editor (KB2251487)	Important

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS09-062	Security Update for Microsoft Visual Studio 2008 (KB972221)	Low

	Office Security Updates	4 security updates are missing.

Security Updates

Score	ID	Description	Maximum Severity
Missing	MS09-043	Security Update for Microsoft Office 2003 Web Components for the 2007 Microsoft Office System (KB947318)	Critical
Missing	3191828	Security Update for Microsoft Office 2007 suites (KB3191828)	Important
Missing	2596904	Security Update for Microsoft Office 2007 suites (KB2596904)	Important
Missing	MS16-004	Security Update for Microsoft Office 2007 suites (KB2881067)	Important

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	949426	Microsoft Office Accounting 2008 UK Service Pack 1 (KB949426)	
Installed	937961	Office 2003 Web Components Service Pack 1 for the 2007 Microsoft Office System	
Installed	949426	Microsoft Office Accounting 2008 US Service Pack 1 (KB949426)	

	SQL Server Security Updates	1 service packs or update rollups are missing.

Update Rollups and Service Packs

Score	ID	Description
Missing	2546951	Microsoft SQL Server 2008 Service Pack 3 (KB2546951)

Current Update Compliance

Score	ID	Description	Maximum Severity
Installed	MS06-061	MSXML 6.0 RTM Security Update (925673)	Critical

	Windows Security Updates	No security updates are missing.

Current Update Compliance

Score	ID	Description	Maximum Severity

Installed	MS15-004	Security Update for Windows Server 2008 R2 x64 Edition (KB3019978)	Important
Installed	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2884256)	Important
Installed	MS15-102	Security Update for Windows Server 2008 R2 x64 Edition (KB3084135)	Important
Installed	MS15-118	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB3097989)	Important
Installed	MS14-046	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2943357)	Important
Installed	MS14-074	Security Update for Windows Server 2008 R2 x64 Edition (KB3003743)	Important
Installed	MS13-079	Security Update for Windows Server 2008 R2 x64 Edition (KB2853587)	Important
Installed	MS15-080	Security Update for Windows Server 2008 R2 x64 Edition (KB3078601)	Critical
Installed	MS16-032	Security Update for Windows Server 2008 R2 x64 Edition (KB3139914)	Important
Installed	MS12-083	Security Update for Windows Server 2008 R2 x64 Edition (KB2765809)	Important
Installed	MS13-007	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2736422)	Important
Installed	MS12-006	Security Update for Windows Server 2008 R2 x64 Edition (KB2585542)	Important
Installed	890830	Windows Malicious Software Removal Tool x64 - August 2017 (KB890830)	
Installed	MS14-072	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2978120)	Important
Installed	MS14-053	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2973112)	Important
Installed	MS11-085	Security Update for Windows Server 2008 R2 x64 Edition (KB2620704)	Low
Installed	MS15-028	Security Update for Windows Server 2008 R2 x64 Edition (KB3030377)	Important
Installed	MS11-075	Security Update for Windows Server 2008 R2 x64 Edition (KB2564958)	Important
Installed	MS15-037	Security Update for Windows Server 2008 R2 x64 Edition (KB3046269)	Important
Installed	MS15-085	Security Update for Windows Server 2008 R2 x64 Edition (KB3071756)	Important
Installed	MS14-064	Security Update for Windows Server 2008 R2 x64 Edition (KB3010788)	Important
Installed	MS16-072	Security Update for Windows Server 2008 R2 x64 Edition (KB3159398)	Important
Installed	MS15-041	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB3037574)	Important
Installed	MS15-097	Security Update for Windows Server 2008 R2 x64 Edition (KB3086255)	
Installed	MS11-024	Security Update for Windows Server 2008 R2 x64 Edition (KB2506212)	Important
Installed	MS14-066	Security Update for Windows Server 2008 R2 x64 Edition (KB2992611)	Critical
Installed	3004375	Security Update for Windows Server 2008 R2 x64 Edition (KB3004375)	
Installed	MS16-021	Security Update for Windows Server 2008 R2 x64 Edition (KB3133043)	Important
Installed	MS13-082	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2861698)	Important
Installed	MS14-007	Security Update for Windows Server 2008 R2 x64 Edition (KB2912390)	Critical
Installed	MS15-071	Security Update for Windows Server 2008 R2 x64 Edition (KB3068457)	Important
Installed	MS16-055	Security Update for Windows Server 2008 R2 x64 Edition (KB3156016)	Critical
Installed	MS16-019	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3122648)	Important
Installed	MS16-055	Security Update for Windows Server 2008 R2 x64 Edition (KB3156019)	Critical
Installed	MS11-030	Security Update for Windows Server 2008 R2 x64 Edition (KB2509553)	Critical
Installed	MS16-014	Security Update for Windows Server 2008 R2 x64 Edition (KB3126587)	Important
Installed	MS14-078	Security Update for Windows Server 2008 R2 x64 Edition (KB2991963)	Moderate
Installed	MS13-004	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2742599)	Important
Installed	MS14-068	Security Update for Windows Server 2008 R2 x64 Edition (KB3011780)	Critical
Installed	MS12-074	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2729452)	Critical
Installed	2984972	Security Update for Windows Server 2008 R2 x64 Edition (KB2984972)	
Installed	MS15-117	Security Update for Windows Server 2008 R2 x64 Edition (KB3101722)	Important
Installed	MS16-087	Security Update for Windows Server 2008 R2 x64 Edition (KB3170455)	Critical

Installed	MS14-009	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2911501)	Important
Installed	MS12-020	Security Update for Windows Server 2008 R2 x64 Edition (KB2621440)	Critical
Installed	MS15-119	Security Update for Windows Server 2008 R2 x64 Edition (KB3092601)	Important
Installed	MS14-039	Security Update for Windows Server 2008 R2 x64 Edition (KB2973201)	Important
Installed	MS12-035	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2604115)	Critical
Installed	MS12-024	Security Update for Windows Server 2008 R2 x64 Edition (KB2653956)	Critical
Installed	MS15-005	Security Update for Windows Server 2008 R2 x64 Edition (KB3022777)	Important
Installed	2841134	Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems	
Installed	MS15-132	Security Update for Windows Server 2008 R2 x64 Edition (KB3108371)	Important
Installed	MS12-054	Security Update for Windows Server 2008 R2 x64 Edition (KB2705219)	Moderate
Installed	MS11-059	Security Update for Windows Server 2008 R2 x64 Edition (KB2560656)	Important
Installed	MS15-084	Security Update for Windows Server 2008 R2 x64 Edition (KB3076895)	Important
Installed	MS16-077	Security Update for Windows Server 2008 R2 x64 Edition (KB3161949)	Important
Installed	MS16-007	Security Update for Windows Server 2008 R2 x64 Edition (KB3108664)	Important
Installed	MS15-038	Security Update for Windows Server 2008 R2 x64 Edition (KB3045685)	Important
Installed	MS13-099	Security Update for Windows Server 2008 R2 x64 Edition (KB2892074)	Critical
Installed	MS15-133	Security Update for Windows Server 2008 R2 x64 Edition (KB3109103)	Important
Installed	MS15-024	Security Update for Windows Server 2008 R2 x64 Edition (KB3035132)	Important
Installed	2973351	Security Update for Windows Server 2008 R2 x64 Edition (KB2973351)	
Installed	MS12-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2758857)	Critical
Installed	MS15-048	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB3023215)	Important
Installed	MS15-088	Security Update for Windows Server 2008 R2 x64 Edition (KB3046017)	Important
Installed	MS15-101	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB3074543)	Important
Installed	MS12-082	Security Update for Windows Server 2008 R2 x64 Edition (KB2770660)	Important
Installed	MS13-090	Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB2900986)	Moderate
Installed	MS15-060	Security Update for Windows Server 2008 R2 x64 Edition (KB3059317)	Important
Installed	MS15-132	Security Update for Windows Server 2008 R2 x64 Edition (KB3108381)	Important
Installed	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2864202)	Important
Installed	MS15-082	Security Update for Windows Server 2008 R2 x64 Edition (KB3075220)	Important
Installed	MS16-007	Security Update for Windows Server 2008 R2 x64 Edition (KB3110329)	Important
Installed	MS12-073	Security Update for Windows Server 2008 R2 x64 Edition (KB2719033)	Moderate
Installed	4034664	2017-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4034664)	Critical
Installed	MS15-090	Security Update for Windows Server 2008 R2 x64 Edition (KB3060716)	Important
Installed	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2868038)	Important
Installed	3042058	Security Update for Windows Server 2008 R2 x64 Edition (KB3042058)	
Installed	MS14-057	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2972100)	Critical
Installed	MS12-012	Security Update for Windows Server 2008 R2 x64 Edition (KB2643719)	Important
Installed	2862152	Security Update for Windows Server 2008 R2 x64 Edition (KB2862152)	
Installed	2871997	Security Update for Windows Server 2008 R2 x64 Edition (KB2871997)	
Installed	MS14-053	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2972211)	Important
Installed	MS15-050	Security Update for Windows Server 2008 R2 x64 Edition (KB3055642)	Important
Installed	2977292	Security Update for Windows Server 2008 R2 x64 Edition (KB2977292)	
Installed	MS12-013	Security Update for Windows Server 2008 R2 x64 Edition (KB2654428)	Critical
Installed	MS15-014	Security Update for Windows Server 2008 R2 x64 Edition (KB3004361)	Important

Installed	MS14-057	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2968294)	Important
Installed	MS12-073	Security Update for Windows Server 2008 R2 x64 Edition (KB2716513)	Moderate
Installed	MS14-046	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2937610)	Important
Installed	MS14-026	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2931356)	Important
Installed	MS00-000	Security Update for Windows Server 2008 R2 x64 Edition (KB2813430)	Moderate
Installed	MS16-082	Security Update for Windows Server 2008 R2 x64 Edition (KB3161958)	Important
Installed	4034733	Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB4034733)	Moderate
Installed	2894844	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2894844)	
Installed	4019112	May, 2017 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Server 2008 R2 for x64 (KB4019112)	Important
Installed	MS15-015	Security Update for Windows Server 2008 R2 x64 Edition (KB3031432)	Important
Installed	MS13-052	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2840631)	Important
Installed	MS12-045	Security Update for Windows Server 2008 R2 x64 Edition (KB2698365)	Moderate
Installed	MS12-020	Security Update for Windows Server 2008 R2 x64 Edition (KB2667402)	Critical
Installed	MS12-036	Security Update for Windows Server 2008 R2 x64 Edition (KB2685939)	Critical
Installed	MS16-033	Security Update for Windows Server 2008 R2 x64 Edition (KB3139398)	Important
Installed	MS13-027	Security Update for Windows Server 2008 R2 x64 Edition (KB2807986)	Important
Installed	MS13-098	Security Update for Windows Server 2008 R2 x64 Edition (KB2893294)	Critical
Installed	MS16-007	Security Update for Windows Server 2008 R2 x64 Edition (KB3109560)	Important
Installed	MS15-080	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 for x64 (KB3072305)	Critical
Installed	MS15-003	Security Update for Windows Server 2008 R2 x64 Edition (KB3021674)	Important
Installed	MS13-015	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2789645)	Important
Installed	MS15-011	Security Update for Windows Server 2008 R2 x64 Edition (KB3000483)	Critical
Installed	MS12-033	Security Update for Windows Server 2008 R2 x64 Edition (KB2690533)	Important
Installed	MS16-019	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3127220)	Important
Installed	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2862330)	Important
Installed	MS11-100	Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2656356)	Critical
Installed	MS13-081	Security Update for Windows Server 2008 R2 x64 Edition (KB2862335)	Important
Installed	MS15-029	Security Update for Windows Server 2008 R2 x64 Edition (KB3035126)	Important

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Password Expiration	Some user accounts (4 of 93) have non-expiring passwords. **User** Invitado christian.ayala pamela.massay temporal1

Administrators	More than 2 Administrators were found on this computer.	
	User	
	GOBERGUAYAS\Administrador	
	GOBERGUAYAS\Administradores de empresas	
	GOBERGUAYAS\TIC	
Windows Firewall	Windows Firewall is disabled and has exceptions configured.	
	Connection Name	**Firewall** / **Exceptions**
	All Connections	Off / Services
	Conexión de área local	Off* / Services*
	Conexión de área local 2	Off* / Services*
	Conexión de área local 3	Off* / Services*
Incomplete Updates	No incomplete software update installations were found.	
File System	All hard drives (1) are using the NTFS file system.	
	Drive Letter	**File System**
	C:	NTFS
Guest Account	The Guest account is disabled on this computer.	
Autologon	Autologon is not configured on this computer.	
Restrict Anonymous	Computer is properly restricting anonymous access.	
Automatic Updates	Updates are automatically downloaded and installed on this computer.	
Local Account Password Test	Password checks are not performed on a domain controller.	

Additional System Information

Score	Issue	Result
	Windows Version	Computer is running Microsoft Windows 7.
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such logoff. Be sure to monitor your event log to watch for unauthorized access.
	Shares	18 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\Windows	Admin Share	NT SERVICE\Tru F, NT AUTHORI RWXD, BUILTIN\Admini RWXD, BUILTIN
Administrativo	c:\Gobernacion\Administrativo	GOBERGUAYAS\TIC - F, GOBERGUAYAS\ADMINISTRATIVO - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario

			GOBERGUAYAS\ - F
C$	C:\	Admin Share	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario
Comunicaciones	c:\Gobernacion\Comunicaciones	GOBERGUAYAS\TIC - F, GOBERGUAYAS\COMUNICACIONES - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
Despacho Principal	c:\Gobernacion\Despacho Principal	GOBERGUAYAS\TIC - F, GOBERGUAYAS\DESPACHO PRINCIPAL - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
Evelyn Ormaza	C:\Gobernacion\Evelyn Ormaza	GOBERGUAYAS\TIC - F, GOBERGUAYAS\evelyn.ormaza - F	GOBERGUAYAS\ - F, NT AUTHOR F, BUILTIN\Adm F, BUILTIN\Usu GOBERGUAYAS\ - F
Financiero	c:\Gobernacion\Financiero	GOBERGUAYAS\TIC - F, GOBERGUAYAS\FINANCIERO - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
Gestion Presidencial	c:\Gobernacion\Gestion Presidencial	GOBERGUAYAS\TIC - F, GOBERGUAYAS\GESTION PRESIDENCIAL - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
Instaladores	C:\Gobernacion\Instaladores	Todos - R, GOBERGUAYAS\TIC - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario
Jefatura Politica	c:\Gobernacion\Jefatura Politica	GOBERGUAYAS\TIC - F, GOBERGUAYAS\JEFATURA POLITICA - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
Juridico	c:\Gobernacion\Juridico	GOBERGUAYAS\TIC - F, GOBERGUAYAS\JURIDICO - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
NETLOGON	C:\Windows\SYSVOL\sysvol\GoberGuayas.local\SCRIPTS	Todos - R, Administradores - F	NT AUTHORITY\ autentificados - BUILTIN\Opers. - RX, BUILTIN\Admini NT AUTHORITY\
Planificacion	c:\Gobernacion\Planificacion	GOBERGUAYAS\TIC - F, GOBERGUAYAS\PLANIFICACION - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuario GOBERGUAYAS\ - F
SYSVOL	C:\Windows\SYSVOL\sysvol	Todos - R, Administradores - F, NT AUTHORITY\Usuarios autentificados - F	NT AUTHORITY\ autentificados - BUILTIN\Opers. - RX, BUILTIN\Admini NT AUTHORITY\ CREATOR OWNE
Secretaria General	c:\Gobernacion\Secretaria General	GOBERGUAYAS\TIC - F, GOBERGUAYAS\SECRETARIA	NT AUTHORITY\ BUILTIN\Admini

SQL Server Scan Results: Instance (default)

Administrative Vulnerabilities

Score	Issue	Result
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	Password Policy	Enable password policy and expiration for the SQL server accounts.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	Sysadmins	More than 2 members of sysadmin role are present.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts should not be members of the local Administrators group or run as LocalSystem.
	CmdExec role	CmdExec is restricted to sysadmin only.
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Folder Permissions	
	Sysadmin role members	BUILTIN\Administrators group is not part of sysadmin role.
	Guest Account	The Guest account is not enabled in any of the databases.
	SSIS Roles	The BUILTIN Admin does not belong to the SSIS roles.
	Sysdtslog	Sysdtslogs90 table does not exist in the Master or MSDB databases

Instance	Service	Account	Issue
(default)	MSSQLServer	SYSTEM	LocalSystem account.
(default)	SQLServerAgent	SYSTEM	LocalSystem account.

Instance	Folder	User
(default)	Internal error.	-

SQL Server Scan Results: Instance MSAS10.MSSQLSERVER

Administrative Vulnerabilities

Score	Issue	Result
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	CmdExec role	CmdExec is restricted to sysadmin only.

Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.	
Folder Permissions	**Instance**	**Folder** / **User**
	MSAS10.MSSQLSERVER	Internal error. / -
Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.	
Sysadmin role members	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Guest Account	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Sysadmins	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Password Policy	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
SSIS Roles	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	
Sysdtslog	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.	

SQL Server Scan Results: Instance MSRS10.MSSQLSERVER

Administrative Vulnerabilities

Score	Issue	Result
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	CmdExec role	CmdExec is restricted to sysadmin only.
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Folder Permissions	**Instance** / **Folder** / **User**
		MSRS10.MSSQLSERVER / Internal error. / -
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.
	Sysadmin role members	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Guest Account	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Sysadmins	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.

	Password Policy	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	SSIS Roles	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Sysdtslog	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.

SQL Server Scan Results: Instance MSSQL10.MSSQLSERVER

Administrative Vulnerabilities

Score	Issue	Result
!	CmdExec role	Error reading registry. If you are scanning a remote computer the Remote Registry service on that computer should be enabled. (13)
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	Folder Permissions	Permissions on the SQL Server and/or MSDE installation folders are not set properly.

Instance	Folder	User
MSSQL10.MSSQLSERVER	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn	\CREATOR OWNER
MSSQL10.MSSQLSERVER	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn	BUILTIN\Usuarios
MSSQL10.MSSQLSERVER	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn	NT SERVICE\MSSQLSERVER
MSSQL10.MSSQLSERVER	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data	\CREATOR OWNER
MSSQL10.MSSQLSERVER	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data	NT SERVICE\MSSQLSERVER
MSSQL10.MSSQLSERVER	C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data	GOBERGUAYAS\christian.ayala

	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem.
	Sysadmin role members	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Guest Account	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Sysadmins	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Password Policy	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	SSIS Roles	

		[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.
	Sysdtslog	[DBNETLIB][ConnectionOpen (Connect()).]No existe el servidor SQL Server o se ha denegado el acceso al mismo.

SQL Server Scan Results: Instance (default) (32-bit)

Administrative Vulnerabilities

Score	Issue	Result
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller.
	Password Policy	Enable password policy and expiration for the SQL server accounts.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode).
	Sysadmins	More than 2 members of sysadmin role are present.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts should not be members of the local Administrators group or run as LocalSystem.
	CmdExec role	CmdExec is restricted to sysadmin only.
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	Folder Permissions	
	Sysadmin role members	BUILTIN\Administrators group is not part of sysadmin role.
	Guest Account	The Guest account is not enabled in any of the databases.
	SSIS Roles	The BUILTIN Admin does not belong to the SSIS roles.
	Sysdtslog	Sysdtslogs90 table does not exist in the Master or MSDB databases

Instance	Service	Account	Issue
(default) (32-bit)	MSSQLServer	SYSTEM	LocalSystem account.
(default) (32-bit)	SQLServerAgent	SYSTEM	LocalSystem account.

Instance	Folder	User
(default) (32-bit)	Internal error.	-

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones have secure settings for all users.

Macro Security No supported Microsoft Office products are installed.

		GENERAL - F	BUILTIN\Usuaric GOBERGUAYAS\ - F
Seguridad Ciudadana	c:\Gobernacion\Seguridad Ciudadana	GOBERGUAYAS\TIC - F, GOBERGUAYAS\SEGURIDAD CIUDADANA - F	GOBERGUAYAS\ CIUDADANA - R AUTHORITY\SY BUILTIN\Admini BUILTIN\Usuaric GOBERGUAYAS\ - F
TIC	c:\Gobernacion\TIC	GOBERGUAYAS\TIC - F	NT AUTHORITY\ BUILTIN\Admini BUILTIN\Usuaric GOBERGUAYAS\ - F
Talento Humano	c:\Gobernacion\Talento Humano	GOBERGUAYAS\TIC - F, GOBERGUAYAS\Talento Humano - F	GOBERGUAYAS\ Humano - F, NT AUTHORITY\SY BUILTIN\Admini BUILTIN\Usuaric GOBERGUAYAS\ - F

Services	Some potentially unnecessary services are installed.		
	Service		**State**
	Servicio de publicación World Wide Web		Running

Internet Information Services (IIS) Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Sample Applications	IIS sample applications are not installed.
	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
	Parent Paths	Parent paths are not enabled.
	MSADC and Scripts Virtual Directories	The MSADC and Scripts virtual directories are not present.
	IIS Lockdown Tool	The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Windows Server 2003 installations running IIS 6.0.

Additional System Information

Score	Issue	Result
	Domain Controller Test	IIS is running on a primary or backup domain controller.
	IIS Logging Enabled	All web and FTP sites are using the recommended logging options.

ANEXO 9

QUALYS® FREESCAN

Vulnerability Scan

29 August 2017 at 21:34

URL : http://zimbra.goberguayas.gob.ec

OWASP Summary : 12 vulnerabilities found
Pages impacted : 7
Vulnerabilities Detected : 12

Risk percentage by scanned pages

0 Pages Scanned
Impacted Pages: 7 (0%)

Impacted Pages by Category

Injection
0 Impacted Pages

Description

OWASP: Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No Injection vulnerabilities were identified with QualysGuard Freescan.

Broken Authentication and Session Management
6 Impacted Pages

QID: 150053
Login Form Is Not Submitted Via HTTPS

http://zimbra.goberguayas.gob.ec/

QID: 150122
Cookie Does Not Contain The "secure" Attribute

http://zimbra.goberguayas.gob.ec/

http://zimbra.goberguayas.gob.ec/;jsessionid=q1r13v753zua18bxjpd4ndhwa?loginOp=relogin&client=socialfox&loginErrorCode=service.AUTH_REQUIRED

http://zimbra.goberguayas.gob.ec/public/launchSidebar.jsp

QID: 150123
Cookie Does Not Contain The "HTTPOnly" Attribute

http://zimbra.goberguayas.gob.ec/

http://zimbra.goberguayas.gob.ec/;jsessionid=q1r13v753zua18bxjpd4ndhwa?loginOp=relogin&client=socialfox&loginErrorCode=service.AUTH_REQUIRED

Description

OWASP: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users identities. Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted. Such flaws may allow some or even all accounts to be attacked. Privileged accounts are frequently targeted. To prevent Broken Authentication and Session Management develop and use a single set of strong authentication and session manage controls.

Cross-Site Scripting (XSS)

Not Checked

Description

OWASP: XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc. To prevent XSS the preferred option is to properly escape all untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL) that the data will be placed into.

No XSS vulnerabilities were identified with QualysGuard Freescan.

Insecure Direct Object References

Not Checked

Description

OWASP: A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. Such flaws can compromise all the data that can be referenced by the parameter. Unless the name space is sparse, it's easy for an attacker to access all available data of that type. To prevent Insecure Direct Object References use per user or session indirect object references. This prevents attackers from directly targeting unauthorized resources. Alternatively include an access control check to ensure the user is authorized for the requested object.

No Insecure Direct Object Reference vulnerabilities were identified with QualysGuard Freescan.

Security Misconfiguration

2 Impacted Pages (Partially verified)

QID: 150085
Slow HTTP POST vulnerability

http://zimbra.goberguayas.gob.ec/

QID: 150086
Server accepts unnecessarily large POST request body

http://zimbra.goberguayas.gob.ec

Description

OWASP: Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application. Such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise. To prevent Security Misconfiguration use repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down, ensure you are applying software patches and upgrades, ensure a strong architecture and good separation and security between components and consider running scans and doing audits periodically.

Sensitive Data Exposure

4 Impacted Pages (Partially verified)

QID: 150053
Login Form Is Not Submitted Via HTTPS

http://zimbra.goberguayas.gob.ec/

QID: 150122
Cookie Does Not Contain The "secure" Attribute

http://zimbra.goberguayas.gob.ec/

http://zimbra.goberguayas.gob.ec/public/launchSidebar.jsp

http://zimbra.goberguayas.gob.ec/;jsessionid=q1r13v753zua18bxjpd4ndhwa?loginOp=relogin&client=socialfox&loginErrorCode=service.AUTH_REQUIRED

Description

OWASP: Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Missing Function Level Access Control

Not Checked

Description

OWASP: Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

No Missing Function Level Access Control vulnerabilities were identified with QualysGuard Freescan.

Cross-Site Request Forgery (CSRF)

Not Checked

Description

OWASP: OWASP notes: a CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim. Attackers can cause victims to change any data the victim is allowed to change or perform any function the victim is authorized to use. To prevent CSRF the preferred option is to include the unique token in a hidden field.

No CSRF vulnerabilities were identified with QualysGuard Freescan.

Using Components with Known Vulnerabilities

Not Checked

Description

OWASP: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

No Using Components with Known Vulnerabilities vulnerabilities were identified with QualysGuard Freescan.

Unvalidated Redirects and Forwards

Not Checked

Description

OWASP: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

No Unvalidated Redirects and Forwards vulnerabilities were identified with QualysGuard Freescan.

ANEXO 10

QUALYS® FREESCAN

Vulnerability Scan

29 August 2017 at 21:34

Endpoint: http://zimbra.goberguayas.gob.ec

Patch Report Summary:

Patches Required: 1
Vulnerabilities Addressed: 1

Type	Patches
	OpenSSH "X SECURITY" Bypass Vulnerability

Vendor ID: **OpenSSH 6.9** Published: –

1 Vulnerabilities Addressed

QID: 38611 OpenSSH "X SECURITY" Bypass Vulnerability

Solution: Users are advised to upgrade to the latest version of the software available.
Refer to OpenSSH 6.9 Release Notes for further information.