



Informe de Trabajo Agosto 2024

# Informe de Trabajo Agosto 2024

# Índice

## Contenido

Objetivo .....	3
Objetivos Específicos .....	3
Alcance .....	3
Tareas Realizadas .....	4
Otras Tareas y gestiones: .....	5
Conclusiones y Recomendaciones .....	6

## Objetivo

Registrar los avances de los proyectos de renovación tecnológica, mejora continua y seguridad de los servicios y plataformas de la Gerencia de Tecnología y Sistemas, además de brindar apoyo en la mantención de la operación diaria de las plataformas institucionales.

## Objetivos Específicos

- Apoyo en ejecución, administración y operación de proyectos en curso dentro de la Gerencia de Tecnología, área de Infraestructura.
- Administrar las instalaciones del Datacenter de SERCOTEC.
- Apoyar en tareas de administración de plataformas como Google Workspace, VMware, Veeam Backup and Replication, entre otras. Elaboración y diseño de los diversos documentos que se requieran.
- Seguimiento a la implementación de los proyectos en elaboración.
- Asistir en la monitorización de plataformas encargadas de la seguridad de la red de Sercotec.

## Alcance

El alcance de los trabajos es ejecutar, administrar y operar las plataformas que componen la infraestructura de la institución y brindar apoyo en los proyectos en ejecución de la Gerencia de Tecnología y Sistemas, en el periodo que comprende el mes de Agosto del año 2024

## Tareas Realizadas

- Se da continuidad a los trabajos de administración y monitorización de ambientes de virtualización productiva y desarrollo bajo las tecnologías de virtualización VMware. Además, se gestionan los recursos de estos entornos de virtualización. Se procede también con las actualizaciones de la plataforma, en base a los parches de seguridad liberados y a la aplicación de medidas de seguridad entregadas por los diversos organismos competentes en la materia.
- Se da continuidad a los trabajos de administración y monitoreo de las diversas plataformas de seguridad implementadas en la organización, incluyendo dentro de estas la seguridad perimetral con los firewalls Sophos XG 430 y Palo Alto PA-850. La seguridad de los usuarios a través de antivirus Sophos Endpoint Protection, la de correos a través de Sophos Email Security.
- Se da continuidad a los trabajos de administración y solución de incidentes sobre la Central Telefonía, basada en Asterisk, brindando apoyo a los distintos requerimientos solicitados por parte de la Mesa de Ayuda.
- Se mantienen las tareas de respaldo de información crítica del negocio a través de la plataforma Veeam Backup and Replication. Estos respaldos se realizan tanto de máquinas virtuales productivas y de desarrollo como de bases de datos, así como también a base de replicas entre el sitio productivo, hacia el sitio de contingencia. También se lleva un control sobre las actualizaciones de dicho sistema de respaldo, con el objetivo de mantener el buen funcionamiento de la plataforma.
- Se da continuidad a las labores de administración de la plataforma Google Workspace en aspectos de administración, configuración y seguridad. Se brinda apoyo a los distintos requerimientos solicitados por la Mesa de Ayuda y se mantiene un contacto constante con la empresa proveedora

para buscar mejoras en el servicio. Se aplican mejoras como la sincronización de directorio a través de Microsoft Entra ID.

- Se da continuidad a las labores de administración de la plataforma Active Directory, abarcando la mantención e implementación de mejoras y buenas prácticas en todos los roles habilitados. Se brinda apoyo a los distintos requerimientos solicitados por la Mesa de Ayuda y el Área de Desarrollo de la Gerencia, con el fin de mantener un ambiente limpio y organizado en el directorio activo. Se mantiene un contacto constante con la empresa proveedora del servicio de soporte de plataformas Microsoft para solucionar incidentes de mayor complejidad y buscar mejoras en dichos servicios.
- Se implementa plataforma SIEM Opensource Wazuh, con el fin de llevar un control interno sobre los servidores y los aplicativos que se ejecutan normalmente dentro de estos, con el fin de monitorear actividades sospechosas dentro de estos. También se implementan distintos tipos de gatilladores de alerta, según su criticidad, así como también los medios de notificaciones de estas, siendo via correo las alertas de categoría media, y por mensajería instantánea, las alertas altas y críticas. Se seguirán implementando mejoras e integraciones a esta plataforma, con el fin de abarcar todas las aristas posibles a nivel de seguridad y cumplimiento.
- Se brinda apoyo para con los proyectos en ejecución y por ejecutar, además de también apoyar con la planificación de los proyectos a presentar en un futuro.

### **Otras Tareas y gestiones:**

- Se brinda apoyo a área de soporte, en materias de control de inventario, gestión de tickets y supervisión de tareas diarias.
- Se brinda asistencia a usuarios con problemas para la conexión a la red VPN.

## Conclusiones y Recomendaciones

Se mantiene un control constante sobre las plataformas administradas, manteniendo siempre un enfoque preventivo en pos de mitigar cualquier incidencia que pudiese suceder. Además de estar siempre en busca de mejoras que puedan traer beneficios al área.

Se mantiene recomendación de repasar las directrices de trabajos al Área de Soporte, en pos de mantener un orden en las plataformas que se han trabajado en el último tiempo.

	<b>Elaborado Por:</b>	<b>Revisado Por:</b>	<b>Revisado y Aprobado Por:</b>
<b>Nombre</b>	Victor Sandoval H.	Claudio Bravo	Iván Quiñones
<b>Cargo</b>	Profesional de Apoyo	Coordinador de Area	Gerente de Tecnología y Sistemas
<b>Fecha</b>	02/Septiembre/2024	02/Septiembre/2024	02/Septiembre/2024
<b>Firma</b>			

Si este documento está clasificado como CONFIDENCIAL, entonces debiera ser utilizado solo con los fines que han sido comunicados por escrito por SERCOTEC en el momento de su entrega. Su contenido no debe ser divulgado total o parcialmente.

