Informe de Trabajo Noviembre 2024

Índice

Contenido

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 noviembre 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 y 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 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 realizan automatizaciones y mejoras a través de scripts en Powershell, con el fin de optimizar ciertas gestiones y realizar automatizaciones. 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 mantiene monitoreo de logs a través del software SIEM Opensource Wazuh, con el fin de visualizar actividades sospechosas dentro de estos. 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 mantiene control y gestión de actualizaciones tanto de usuarios, a través de la herramienta System Center Configuration Manager, así como también de servidores Microsoft y Linux de manera manual y controlada. Se instalan parches de seguridad mensuales liberados para ambas distribuciones y también se lleva control de las actualizaciones de los parches tipo Zero Day.

- Se implementa servicio de monitoreo con aplicación Grafana, con el fin de llevar cuenta de los consumos de las bases de datos dentro del Clúster SQL, con el fin de gestionar de manera oportuna casos de sobreconsumo, exceso de consultas, fallas en las Query. También se comienza a evaluar otros tipos de monitoreo, como el Heartbeat de los sitios expuestos,

control de movimiento en las cuentas con altos privilegios en plataformas internas, control sobre las UPS, supervisión de WAF, entre otros.

- 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.

- Se brinda apoyo a otra Gerencia, con proyecto de sistema de tickets para proyecto Sustentabilidad.

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 trabajo en el último tiempo.

	Elaborado Por:	Revisado Por:	Revisado y Aprobado Por:
Nombre	Victor Sandoval H.	Claudio Bravo	Iván Quiñones
Cargo	Profesional de Apoyo	Coordinador de Area	Gerente de Tecnología y Sistemas
Fecha	02/Diciembre/2024	02/Diciembre/2024	02/Diciembre/2024
Firma	Victor Sandoval Profesional De Área RUT: 17816180-6 Servicio De Cooperacion Tecnica Firmado el 01 de diciembre del 2024 a las 15:46 Hrs.	Claudio Bravo Gomez Profesional De Área RUT: 17256738-K Servicio De Cooperacion Tecnica Firmado el 01 de diciembre del 2024 a las 15:50 Hrs.	**Ivan Quiñones Bastías** Gerente Tecnología y Sistemas SERVICIO DE COOPERACION TECNICA