PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIVERSIDAD DE CALDAS

CONTEXTO Y JUSTIFICACIÓN

Los grandes volúmenes de información institucionales se originan desde diversas fuentes y con estándares tecnológicos heterogéneos -en hardware, software, comunicaciones- que requieren de una infraestructura de red adecuada, funcional y confiable para su transmisión y almacenamiento.

En el caso de la Universidad de Caldas, las soluciones de conectividad y servicios informáticos fueron diseñadas fundamentalmente para soportar aplicaciones de procesamiento de datos que funcionan en un servicio de transporte operativo pero que no han sido rigurosas en parámetros de QoS (calidad del servicio) y CyberSec (ciberseguridad). El crecimiento exponencial de nuevos servicios y aplicaciones -para los cuales no se hizo una planeación adecuada- ha desencadenado en un conjunto de dificultades en la operación de la red y en la gestión de la seguridad de la información, elementos que han estado en una baja y arriesgada prioridad en el dimensionamiento tecnológico institucional. En el marco de las TI se hace necesaria la implementación de estrategias de seguridad para preservar los servicios disponibles y garantizar la confidencialidad e integridad de los datos en las aplicaciones. Existen algunos estándares de seguridad informática que sugieren -como primera medida- realizar análisis de vulnerabilidades para responder corrigiendo posibles fallos y apuntando a modelos preventivos. Estos esfuerzos son inocuos, si en este mismo sentido, la alta dirección no está involucrada y comprometida con la implementación de un Sistema Integral de la Seguridad de la Información.

El presente documento pretende exponer una serie de lineamientos para implementar las mejores prácticas de Seguridad Informática en la Universidad de Caldas, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales.

SEGURIDAD PERIMETRAL

En la Universidad de Caldas se encuentra implementada una solución en alta disponibilidad de Firewall UTM (Unified Threat Management) que contribuye a la seguridad perimetral de los datos, aplicaciones, servicios, servidores y usuarios finales. La solución Fortigate fue configurada para controlar el tráfico bidireccional entre la red de la Universidad de Caldas e internet, evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet y examinar todos los paquetes de datos que entren o salgan de la red local, bloqueando aquellos que no cumplen los criterios de seguridad especificados. Los dispositivos encargados de estas tareas son dos Fortigate, con características completas de UTM (Gestión Unificada de Amenazas) incluyendo firewall, IPS (Sistemas de Prevención de Intrusos), Antivirus, AntiSpam, VPN, Filtrado Web y control de Aplicaciones. Adicionalmente se cuenta con un Fortianalyzer para el análisis de tráfico y la generación de reportes. El análisis de estos reportes lleva a la detección de fallas de seguridad e intrusiones frustradas, además los servicios de subscripción Fortiguard proveen conexión y actualización a las bases de datos propietarias para Antivirus, Prevención de Intrusiones, Filtrado Web, Antispam y Control de aplicaciones.

En capa lógica, se cuenta con segmentación de dominios de broadcast a través de VLANs conectadas a los diferentes puertos del Firewall, procurando controlar el tráfico de cada subred de acuerdo al rol de grupos de usuarios/máquinas: Equipos activos, administrativos, estudiantes, Innovación, oficina de sistemas, almacenamiento, vigilancia, telefonía y Wireless.

Para la conectividad WAN la Universidad tiene un canal dedicado, dividido en 500 Mbps comerciales y 500 Mbps para uso Académico e investigativo, contratados con Telefónica - RENATA (Red Nacional Académica de Tecnología Avanzada) y vinculados a un enrutador Cisco que realiza la conmutación de forma transparente de acuerdo al destino del paquete enviado, si se trata de una petición hacía uno de los sitios de la red Renata, la navegación se realiza a través del canal académico de 500 Mbps y si se trata de una solicitud hacía una página comercial, se utiliza el otro canal de 500 Mbps. Debido a las necesidades actuales de la institución, se hace necesario aplicar traffic shapers a las políticas de navegación de las redes, así como filtros web y controles de aplicaciones para cada VLAN, con el fin de optimizar la seguridad y el uso del canal.

RED

La red LAN de la Universidad de Caldas cuenta con un switch de Núcleo 3Com, donde convergen las conexiones de los servidores, los switches de distribución de las diferentes sedes y los equipos de seguridad perimetral, formando una topología en estrella extendida con centro en el switch de núcleo, adicionalmente operan varias VLANs que segmentan la red a nivel lógico.

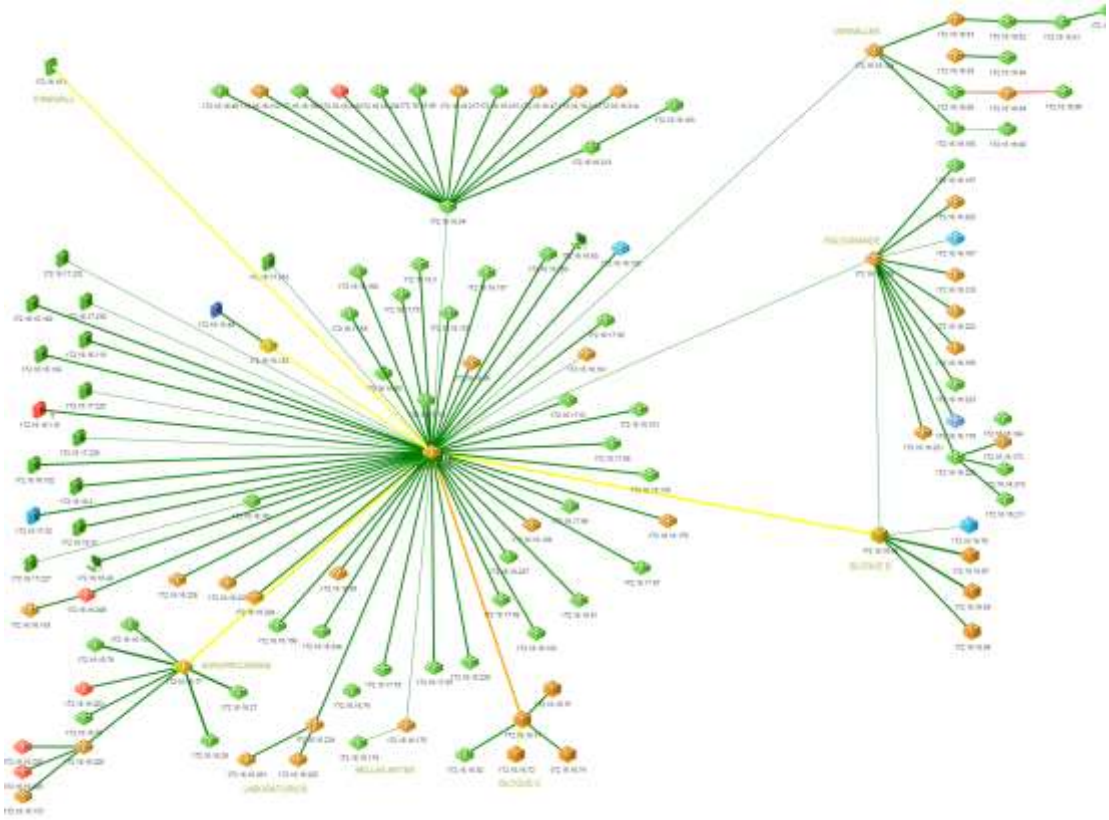

Figura 1. Diagrama topológico de red - Dispositivos activos

De la mano de cualquier adquisición o mejora a nivel técnico, es importante implementar políticas en el manejo de los recursos tecnológicos, para brindar apoyo y orientación a los funcionarios, docentes y estudiantes respecto a la seguridad de la información, acorde a las necesidades y requisitos de la institución.

TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que los equipos informáticos de la Universidad soportan la nueva versión de IP.

SERVIDORES

Bajo la administración de la oficina de sistemas existen 2 enclosure Dell, 5 servidores de almacenamiento NAS y 1 sistema SAN. En dos Blade del Enclosure se encuentra implementado el clúster de bases de datos, donde se alojan las instancias de Gestión Humana y Registro académico.

En los otros 10 servidores se encuentran hospedadas 27 máquinas virtuales, con sistemas operativos Windows y Linux, administradas con Hyper-V. Estas máquinas incluyen los entornos de producción y pruebas de los sistemas de información institucionales, los controladores de dominio y toda la Suite System Center.

APLICACIONES Y BASES DE DATOS

El análisis de aplicaciones conectadas es primordial para poder establecer posibles fallos de implementación que conducen a vulnerabilidades en cualquier de las capas de las arquitecturas desplegadas.

Los puntos de control más relevantes que se verificarán estarán concentrados en: validar desbordamientos de pilas, verificación de cadenas y secuencias inválidas, datos inconsistentes de control, inspección de Metadatos que conducen a fugas de información, errores de validación, errores de procesamiento, entre otros.

Las bases de datos actuales están instaladas en dos nodos redundantes, en este momento se están ejecutando actividades como: Actualización mensual de las instancias de pruebas, creación de usuarios y esquemas, asignación y revocatoria de permisos en los usuarios, mantenimiento de Tablespaces, detección y eliminación de bloqueos, copias de seguridad diarias, instalaciones periódicas de nuevas actualizaciones de software.

Existen un número importante de aplicaciones desarrolladas y contratadas que tienen vínculo con otros gestores de bases de datos relacionales y servidores de despliegue donde es inminente generar un estudio de seguridad multicapa para identificar riesgos potenciales.

También se deben contemplar otras actividades como: documentación de estadísticas de rendimiento, incluyendo los posibles cambios de configuración y sincronización que esto conlleva y realizar afinamientos periódicos con su correspondiente documentación, para un rendimiento óptimo de la base de datos.