GIDT

Plan de Tratamiento del Riesgo

Grupo Funcional de Seguridad Información
UNAD
29/03/2021

PLAN DE TRATAMIENTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN 2021

De acuerdo con el análisis de riesgos tecnológicos generales y específicos asociados a tecnologías, que se pueden presentar en la infraestructura tecnológica administrada por la GIDT-PTI, a continuación, se presenta el plan de tratamiento de riesgos de seguridad de la información a desarrollar durante el año 2021:

1. Emitir boletines informativos publicados en la sección de tecnología en el portal institucional.

2. Por medio de una política de directorio activo, desplegar imágenes tipo papel tapiz relacionadas con tips de seguridad de la información a todas las estaciones de trabajo y servidores de la UNAD.

3. Emitir boletines de seguridad sobre vulnerabilidades asociadas a los sistemas operativos de estaciones de trabajo y servidores de la UNAD, como también recomendaciones a la comunidad Unadista con temas relacionados al fraude e ingeniería social a través del correo institucional.

4. Emitir los certificados digitales de seguridad SSL a los sistemas de información de la UNAD que funcionan en la web.

5. Implementar, configurar y puesta en marcha de la nueva consola Sophos Antivirus Intercept X Advanced for Server with EDR como mecanismo de detección de malware y virus informático en la red LAN de la UNAD.

6. Aseguramiento a nivel de hardening de la infraestructura nueva de servidores Windows Server.

7. Aseguramiento a nivel de ransomware a nivel de estaciones de trabajo y equipos de cómputo.

8. Ejecución diaria de copias de respaldo de la información con un sistema automatizado que permite optimizar el proceso de ejecución.

9. Generar conciencia a la comunidad Unadista relacionadas con temas de seguridad de la información.

10. Realización de auditorías aleatorias a los equipos de los usuarios para comprobar el software instalado de forma no autorizada.

11. Validación de PQR desde el grupo de seguridad de la información cuando existen requerimiento de instalación de algún tipo de software en particular.

12. Implementar controles en la plataforma de seguridad del Firewall que permitan monitorear el buen uso del canal web institucional, configurar de la mejor manera reglas para la restricción de puertos en los activos de la Universidad (Servidores, Core, Aplicaciones en Producción).

13. Monitoreo en tiempo real del uso no autorizado de la Marca y el Logo de la Universidad a través de herramientas especializadas diseñadas para tal fin.

14. Auditorias forenses sobre casos de suplantación de identidad a docentes y estudiantes, y fraudes académicos que ocurran en la plataforma de campus virtual.

15. Análisis de vulnerabilidades y Hacking Ético sobre aplicaciones de misión crítica en producción.

16. Seguimiento de las Políticas Marco de Referencia del Sistema de Gestión de Seguridad de la Información (SGSI) y la reglamentación de uso de los servicios de tecnología.