UNIVERSIDAD
SIMÓN BOLÍVAR

Informe de Auditoría Interna

Auditoría a la Gestión de las Tecnologías de la Información - TI

Febrero de 2023

Contenido

1. Objetivo general de la auditoría

Esta auditoría tiene como finalidad la verificación del cumplimiento del marco normativo externo e interno de la Universidad, considerando la gestión de riesgos, la ética y las mejores prácticas administrativas con el fin de examinar la efectividad y eficacia de los controles establecidos para mitigar los riesgos asociados a la gestión de TI.

2. Objetivos específicos

1) Conocer y entender los procedimientos que se llevan a cabo en la Universidad para la gestión de la administración, preservación y protección de la información de la Universidad Simón Bolívar.

2) Comprobar el cumplimiento normativo y regulatorio ante entes de control interno y externo en temas de protección de datos y activos de información.

3) Verificar la eficacia de los controles establecidos para mitigar los riesgos del proceso.

4) Comprobar la seguridad informática aplicada a través de mecanismos de control para la identificación y contención de ataques cibernéticos y su materialización.

5) Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de estos.

6) Evaluar la forma como se administran los dispositivos de almacenamiento básico del área de Informática.

7) Evaluar el control que se tiene sobre el mantenimiento y las fallas de las PCs institucionales.

8) Verificar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro de la Dirección de TI.

9) Revisar los procedimientos existentes sobre seguridad física con respecto a instalaciones, personal, equipos, documentación, back-ups, pólizas y planes de contingencias.

10) Comprobar si los planes de seguridad son evaluados periódicamente.

11) Evaluar los procedimientos para asignación y retiro de claves de acceso.

3. Alcance de la Auditoría

Esta auditoría comprende la verificación del cumplimiento de la políticas, normas y procedimientos relacionados con la gestión del proceso de TI en la sede de Barranquilla, y valorar la efectividad de los controles establecidos para garantizar la seguridad de: la información, los equipos, los controles de seguridad de acceso y modificación de bases de datos e información, la confidencialidad, los controles de autenticación por usuario entre otros, así como verificar la oportunidad y eficiencia del mantenimiento de equipos que se presta a las diferentes áreas de la Universidad.

4. Descripción de las Actividades

Durante la realización de la auditoría se efectuaron las siguientes actividades:

1) Revisión de la normatividad externa e interna y otros documentos asociados en el desarrollo del subproceso auditado, los cual se relacionan a continuación:

   Normatividad y otros documentos

   - Ley estatutaria 1581 de 2012- Protección de datos personales.
   - Política Integral de Tecnologías de la Información
   - Acuerdo 001 de 2020, Política de tratamiento de la Información Universidad Simón Bolívar.
   - Reglamento Estudiantil de la Universidad Simón Bolívar.
   - Reglamento Interno de la Universidad Simón Bolívar.
   - Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
   - Ley de Protección de Datos Personales o Ley 1581 de 2012
   - Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 Tecnología De La Información. Técnicas de Seguridad. Sistemas De Gestión De La Seguridad De La Información.
   - Norma Técnica Colombiana GTC-ISO-IEC 27002:2015. Tecnología de la Información.
   - Reglamento de Propiedad Intelectual. Acuerdo No. 59 DE 2021.
   - CONPES 3854; Lineamientos de seguridad digital del Consejo Nacional de Política Económica y Social República de Colombia, Departamento Nacional de Planeación
   - Decreto 1008 de 2018, se define la política de Gobierno Digital, por el cual se establecen los lineamientos generales de la política de Gobierno Digital
   - CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
   - CONPES 3854 de 2016 Política Nacional de Seguridad digital.

2) Análisis de los procedimientos y otros documentos asociados a la Gestión de TI.

   - CP-GT-01 Gestión de TI.
   - P-GT-01 Procedimiento mantenimiento equipos de cómputo
   - P-GT-02 Procedimiento para el otorgamiento modificación o retiro de acceso a usuarios del sistema de Información.
   - P-GT-03 Procedimiento para la generación y restauración de copias de seguridad o Back up.
   - P-GT-07 Procedimiento Protección de Código Malicioso.
   - P-GT-08 Procedimiento Aseguramiento de Servicios en la Red.
   - P-GT-09 Procedimiento para el Mantenimiento de Equipos de Cómputo del Laboratorio de Genética.
   - P-GT-10 Procedimiento Generación de Back up y Restauración de la Información en KACTUS o SEVEN.
   - P-GT-11 Procedimiento Atención de Incidencias y Requerimientos KACTUS o SEVEN.
   - P-GT-12 Procedimiento para la gestión de cuentas de usuario en KACTUS o SEVEN.
   - P-GT-13 Procedimiento para la gestión de requerimientos de recursos y soluciones tecnológicas.

3) Solicitud de información a la Dirección de TI sobre:

- Base de Usuarios de información a nivel general con la asignación de usuarios, roles, perfiles y permisos (incluyendo desactivaciones, bloqueos, inhabilitaciones correos electrónicos deshabilitados, todos con sus respectivas fechas) a septiembre de 2022.
- Pólizas de garantías para la protección de inventarios de TI (hardware).
- Programas de mantenimiento preventivo de equipos de cómputo realizados durante el año 2022.
- Políticas de operación y uso de equipos.
- Políticas de seguridad de la información.
- Listado de controles de acceso al sistema.
- Inventario de equipos de cómputos, tablets, con su asignación de usuarios, licencias, antivirus a septiembre de 2022.
- Listado de copia temporal de Backups, con los periodos de copia de respaldo durante el año 2022.
- Listado maestro de registros con el personal involucrado en la generación de Backups.
- Información de las hojas de vida de los equipos de redes.
- Relación de equipos dados de baja realizados durante los años 2021 y 2022, con sus respectivos soportes.
- Protocolo de acceso a las bases de datos y relación de los encargados del tratamiento de datos personales según su rol en la Universidad.
- Listado de equipos otorgados a los estudiantes con calidad de préstamo con ocasión de la pandemia 2020 -2021, sin reintegrar.
- Listas de chequeo para el alistamiento de los computadores de la Institución

4) Reunión de apertura del proceso de auditoría con el personal de la Dirección de Tecnologías de la Información.

5) Identificación de los controles clave del subproceso.

6) Muestreo selectivo para verificación de efectividad de los controles diseñados para la mitigación de los riesgos.

7) Verificación de inventario de equipos de cómputo y de redes, mediante técnica de muestreo aleatorio.

8) Reuniones con los diferentes responsables asignados para aclaración de inquietudes.

9) Validación de los resultados de la auditoría con los diferentes responsables del suministro de información, análisis de las causas y controles efectuados para mitigar los riesgos asociados.

5. Aspectos Positivos

En el proceso de la Gestión de Tecnologías de la Información se destacan los siguientes aspectos positivos:

- Existencia de procedimientos documentados disponibles en el Sistema de Gestión de Calidad (ISOTools).

- Segregación de funciones y asignación de controles para el acceso a los sistemas tecnológicos y/o Información.

- Compromiso del área por el mejoramiento permanente de la calidad de la información y la prestación del servicio.

- Protección de los inventarios de TI mediante póliza de garantía de todo riesgo renovada anualmente.

- Seguridad en el acceso a las instalaciones de la oficina de TI, a través de sistema digital, que asegura la protección de activos y el ingreso de personal no autorizado según Norma Técnica Colombia NTC27002.

- Control de acceso a los campus universitarios mediante reconocimiento facial.

6. **Oportunidades de mejora**

- Formalizar y socializar los anexos de las políticas de seguridad y privacidad de la información.

- Cumplir oportunamente el procedimiento establecido para el reporte de novedades de controles de accesos y perfiles del personal.

- Ingresar al procedimiento establecido, la actividad de comunicación previa a los líderes de las áreas, el programa de mantenimiento semestral de equipos.

- Verificar la instalación del plugin FusionInventory para cada nuevo equipo o aquel que presente alguna novedad (mantenimiento, cambio de usuario, entre otros), con el fin de tener un monitoreo completo en tiempo real de los equipos de la institución.

- Actualizar la información al 2023 de los equipos sin devolver por parte de los estudiantes y realizar las gestiones pertinentes para la recuperación de estos. Para aquellos que soliciten la ampliación de plazo de préstamo, aplicar el criterio empleado para este proceso y articular con el sistema SIA esta información dando cumplimiento a lo establecido en el reglamento estudiantil que para matricularse o graduarse deben encontrarse a paz y salvo con la Universidad por todo concepto.

- Actualizar en el sistema de información de helpdesk GLPI las novedades de los equipos de red para el monitoreo de estos en tiempo real.

- Realizar periódicamente la inspección y mantenimiento de todos los extintores bajo su custodia con carga al día y lista para su uso, para así evitar contratiempos en caso de requerirlos ante una eventualidad.

- Inspeccionar los tableros Multi-Breakers para que tengan sus elementos de protección y estén dispuestos en sitios de fácil acceso y manipulación, sin obstrucción por elementos que restrinjan su operatividad.

7. Conclusiones

Como resultado de la auditoría se puede concluir que la Universidad:

- ✓ Cuenta con procedimientos claros para una adecuada Gestión de la Dirección de TI.
- ✓ Ha identificado los principales riesgos y se ha establecido controles para mitigar la ocurrencia de ellos.
- ✓ Dispone de herramientas tecnológicas adecuadas para soportar la operación y la protección de equipos.
- ✓ Dispone de personal comprometido con funciones claras a las cuales se les ha asignado roles y perfiles de acceso a los sistemas de información.

Sin embargo, se encuentran aspectos por mejorar los cuales se relacionaron en el numeral anterior.

Cabe destacar que por la importancia que tienen los sistemas de información en la Gestión de la Universidad, se debe continuar fortaleciendo esta área con la contratación de talento humano y asignación de recursos para responder a las múltiples demandas que tiene la academia y la administración.