POLÍTICA PARA LAS COPIAS DE RESPALDO

Contenido

1. Propósito de la política

Establecer los lineamientos para la copia y la recuperación de la información que se encuentra almacenada en los servidores UNAB que soportan las actividades de misión crítica y de sus aplicaciones de apoyo, de tal manera que ante la ocurrencia de un desastre o falla de la infraestructura de hardware y software, se pueda realizar la recuperación de los servicios sin pérdidas de información.

2. Alcance

El presente documento aplica a los administradores de servidores de la UNAB y cubre la información compuesta por todos los datos personales de estudiantes, empleados, proveedores (personas naturales) o de cualquier otro tipo de información pública, interna, confidencial o secreta que sea almacenada en forma digital.

3. Copia de la información de los servidores

3.1 Servidores que se deben incluir en la copia

Para las actividades de copias de seguridad se deben incluir todos aquellos servidores que estén bajo la administración directa de TIC UNAB y que contengan información que sea consultada por usuarios internos o externos de la organización. No se incluyen los equipos que son albergados en el Datacenter como parte de un contrato de arrendamiento de espacio.

3.2 Detalle de la copia

La copia que se debe realizar de cada uno de los servidores debe permitir la reconstrucción completa del mismo, es decir; se debe copiar la información de la aplicación, los ejecutables de la aplicación y el sistema operacional del servidor. Para el caso de las bases de datos, la copia debe incluir las transacciones que se realizan en la misma hasta el momento de la copia, de tal modo que sea posible reconstruir la información de forma consistente y precisa.

3.3 Copia de aplicaciones de apoyo o soporte a las aplicaciones de misión crítica

Los servidores que contienen aplicaciones de apoyo como DHCP, Proxys, DNS, LDAP etc, deben ser copiados en forma completa, es decir; se debe incluir en la copia la información del sistema operacional y la aplicación, de tal modo que en caso de falla el servicio se pueda recuperar rápidamente con mayor estabilidad.

3.4 Periodicidad de la copia

Las copias de respaldo se deben realizar diariamente.

3.5 Contención de las copias

El número de copias consecutivas antes de iniciar el borrado de las mismas debe ser de al menos 30 días.

3.6 Pruebas de recuperación

Las copias de seguridad deben ser recuperadas de oficio para verificar la confiabilidad de las mismas, por lo tanto, el responsable designado por la dirección de Tecnologías de Información y Comunicaciones - TIC elegirá de forma aleatoria un servidor para realizar el proceso de recuperación completa de la información del mismo. Las pruebas de recuperación se deben realizar como mínimo 2 veces al año 1 en cada semestre.

3.7 Copias Externas

Para proteger la información ante desastres se debe generar una copia total de los servidores que permita recuperar la infraestructura después de sufrir una pérdida total de la misma. Esta copia debe almacenarse en forma segura en un lugar alejado del Datacenter de la organización. Estas copias deben mantenerse actualizadas con una frecuencia igual o menor a 1 día.

3.8 Copias a Disco

Como una medida adicional para proteger la información ante desastres se debe generar una copia total de los servidores a discos, esta copia no tendrá contención, será una copia única y diaria de la información y se utilizará como una opción de acceso rápido para recuperación de la información.

4. Copia de información de los equipos de cómputo de los usuarios UNAB

El almacenamiento de la información de las estaciones de trabajo asignadas a los usuarios UNAB se regirá según lo establecido en el documento “Política para la clasificación y almacenamiento de la información física y digital”.

Declaración Final

Esta política fue creada por la Oficina de Seguridad de la Información y revisada por el Comité de Tecnología UNAB. Cada año o en el momento en que se requiera, se verificará la legislación y normas que apliquen en el entorno en el que se desenvuelve la organización para mantenerla actualizada.