# DEPARTAMENTO DE PROCESAMIENTO DE DATOS DE LA DIRECCIÓN GENERAL FINANCIERA

## POLÍTICA DE SERVICIOS DE INFRAESTRUCTURA INFORMÁTICA -InfraDPD-

| | |
|---|---|
| Código: | DPD-R-POL-01 |
| Versión: | 1.0 |
| Fecha de la versión: | junio de 2026 |
| Creado por: | Coordinación de Redes y Comunicaciones |
| Aprobado por: | Jefatura del DPD |
| Alcance: | Todo el personal y sistemas que utilice la Plataforma InfraDPD |
| Nivel de confidencialidad: | Público |
| Firma y Sello | |

# Política de servicios de infraestructura informática InfraDPD

La presente política rige el uso de los servicios de infraestructura informática que brinda el Departamento de Procesamiento de Datos de la Dirección General Financiera (DPD-DGF) a la comunidad universitaria en caso de ser solicitados, analizados y aprobados.

La versión más reciente que sea elaborada por este Departamento es la que estará vigente para los solicitantes de las Unidades o Dependencias (UoD) de la Universidad a las que se les aprueben recursos.

Al hacer uso de los servicios de infraestructura informática (InfraDPD) la UoD está aceptando la última versión de la política.

Toda información y datos almacenados o procesados en los servidores bajo ningún concepto puede ser usada para otros fines que no sean los otorgados por la constitución política de la República, las leyes y reglamentos internos de la Universidad.

## 1. CONDICIONES

**a.** La infraestructura informática aprobada debe ser utilizada únicamente para los fines de la Universidad.

**b.** En el Manual de Normas y Procedimientos de este Departamento y en su sitio web https://dpd.usac.edu.gt, se estipulan los requisitos vigentes para solicitar recursos de infraestructura informática. Ver Anexo A.

**c.** Los servicios de infraestructura informática están sujetos a un análisis y aprobación del proyecto presentado.

## 2. OBJETIVOS

Establecer los lineamientos, responsabilidades y estándares técnicos para el aprovisionamiento, gestión y operación de los servicios de infraestructura virtualizados en la plataforma InfraDPD. Se enfatizan la confidencialidad, integridad y disponibilidad de la información, así como la estabilidad y seguridad del entorno de virtualización que utilice el DPD.

## 3. ALCANCE

Esta política aplica a todos los servidores virtuales (VMs), contenedores (LXC o de otro tipo) y aplicaciones desplegados en InfraDPD.

El personal encargado de la administración del hipervisor del DPD y el personal responsable de la UoD de que administra las VMs y LXC.

## 4. DEFINICIONES

**DPD**: Departamento de Procesamiento de Datos de la Dirección General Financiera.

**InfraDPD**: Servicio interno de infraestructura virtualizada que brinda recursos de cómputo a la Universidad.

**LTS** (*Long Term Support*): versión de software con soporte extendido garantizado por el fabricante.

**Ciclo de vida**: etapas desde el despliegue hasta la retirada (EOL - *End of Life*) del sistema.

**Contenedor LXC**: Sistema operativo ligero virtualizado a nivel de sistema operativo del hypervisor.

**Máquina Virtual VM**: Sistema operativo completo virtualizado con hardware emulado.

**UoD**: Unidad o Dependencia de la Universidad de San Carlos de Guatemala.

**Snapshot**: Instantánea del un contenedor o una máquina virtual para marcar un punto de restauración en el tiempo.

**Ransomware**: Software malicioso (malware) diseñado para bloquear el acceso a un sistema informático o datos, por medio de cifrado de archivos con el fin de extorsionar a la víctima para que pague un rescate, generalmente en criptomoneda.

# 5. ESTÁNDARES DE DESPLIEGUE Y CONFIGURACIÓN

## a. Principios generales

**Seguridad por diseño**: toda nueva instancia debe desplegarse con configuraciones seguras por defecto.

**Mínimo privilegio**: toda nueva instancia o aplicaciones debe seguir el principio de mínimo privilegio.

**Minimización de superficie de ataque**: solo se habilitarán servicios y puertos estrictamente necesarios.

**Cumplimiento de ciclo de vida**: ningún sistema operará fuera de su período de soporte oficial.

**Responsabilidad compartida**: El DPD provee la plataforma segura, con conectividad y exposición desde y hacia internet según corresponda; la UoD solicitante designa encargados, quienes son responsables de la seguridad de sus sistemas operativos invitados, de sus bases de datos, del lenguaje de programación, aplicaciones y de la paquetería instalada.

## b. Requisitos de actualización y parcheo

**Actualización obligatoria**: todos los contenedores y VMs deben mantenerse actualizados con los últimos parches de seguridad disponibles dentro de su ciclo de vida LTS. Esto es responsabilidad de los encargados de la UoD.

**Frecuencia**: parches de seguridad críticos: máximo 72 horas tras su publicación.

**Actualizaciones menores**: máximo 15 días.

**Verificación**: El equipo de Infraestructura realizará auditorías aleatorias para verificar el estado de parches. Los sistemas desactualizados serán aislados automáticamente.

**Servicios no planificados**: En caso que la UoD necesite ampliar sus servicios a través del recurso asignado y esto requiera instalación de más paquetería, apertura o exposición de puertos (aunque sea de manera interna), debe ser solicitado y autorizado por este Departamento.

## c. Gestión del ciclo de vida

**Monitoreo de EOL**: El encargado de la UoD debe estar al tanto de las fechas del fin del soporte del ciclo de vida (EOL) de cualquier sistema operativo desplegado.

**Plan de migración**: El encargado de la UoD debe planificar y ejecutar la migración a una nueva versión LTS antes de la fecha de EOL. Para ello puede solicitar al DPD un *snapshot* de su recurso para tener un punto de restauración.

**Retiro forzoso**: si no se realiza la migración un mes antes de la fecha de EOL, el sistema será desconectado de la red. La UoD deberá contactar al DPD comprometiéndose con la migración en un tiempo razonable DPD procederá a conectar el recurso.

**Eliminación forzosa**: Si no se reciben notificaciones por escrito sobre la actualización pasado el EOL de parte del responsable o la UoD, luego de un mes calendario el recurso será considerado en abandono, por lo que será eliminado de manera permanente y también los backups relacionados.

## 6. GESTIÓN DE ACCESOS Y AUTENTICACIÓN

**Usuarios root/Admin**: el acceso root directo está prohibido en sistemas invitados. Se debe utilizar un usuario con privilegios sudo y auditoría de comandos.

**Autenticación al hypervisor**: el acceso a la plataforma de gestión requiere credenciales únicas y MFA. El uso de cuentas compartidas está estrictamente prohibido.

**Gestión de claves**: el uso de par de llaves SSH es obligatorio para el acceso remoto. Las contraseñas en texto plano están prohibidas. La llave privada y la contraseña de acceso será enviada por medio de correo institucional con dominio @usac.edu.gt debidamente cifrada con PGP.

## 7. RESPALDO Y RECUPERACIÓN

**Política de respaldo de infraestructura**: Todos los sistemas críticos deben tener respaldos automáticos configurados en el hypervisor junto a la herramienta de respaldo.

**Tipos de respaldo**: Incremental y completo

**Frecuencia**: Mínimo semanal para el respaldo incremental y mensual para el completo.

**Pruebas de restauración**: Se realizarán pruebas de restauración trimestralmente para garantizar la integridad de los backups de los equipos súper críticos.

**Retención**: Los respaldos incrementales se conservan las últimas 4 semanas y los últimos 3 mensuales. Los respaldos completos se conserva el último anterior.

**Política de respaldo de aplicaciones y DB**: El responsable de la UoD a cargo de los recursos de cómputo debe realizar backups de aplicaciones y base de datos para mantenerlos fuera de línea.

## 8. MONITOREO Y AUDITORÍA

**Logs**: Todos los sistemas deben enviar sus logs de seguridad (syslog, auth.log, syslog de aplicaciones) a un servidor centralizado de logs (SIEM).

**Alertas**: Se configurarán alertas automáticas para:

Intentos de acceso fallidos.

Cambios en configuraciones críticas.

Fallos en servicios de actualización.

Detección de versiones EOL.

**Auditorías**: Se realizarán revisiones aleatorias del cumplimiento de esta política.

## 9. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de esta política, especialmente en lo referente a la falta de actualizaciones o el uso de versiones sin soporte o instalación de paquetería con otros propósitos que el autorizado, resultará en:

- Aislamiento inmediato del sistema afectado de la red.
- Notificación formal al responsable del servicio y a su supervisor jerárquico de la UoD.
- Suspensión temporal del servicio hasta la remediación.

- Sanciones disciplinarias según las leyes y reglamentos de la Universidad de San Carlos de Guatemala.

## 10. REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

Esta política será revisada anualmente o cuando ocurran cambios significativos en la plataforma de virtualización, en las distribuciones soportadas o en la normativa de seguridad aplicable.

Los usuarios de la infraestructura pueden solicitar por escrito una copia digital de la versión de la política más reciente.

La versión más reciente está disponible en https://dpd.usac.edu.gt.

# 11. ANEXO A

## Requisitos

A continuación se presentan los requisitos para solicitar los recursos.

1. La Unidad o Dependencia (UoD) en oficio formal digital solicita recursos de cómputo virtualizado. Presenta al trabajador universitario identificado como responsable pleno consignando la siguiente información:
    - **a.** Nombre completo.
    - **b.** Registro de personal y CUI.
    - **c.** Email institucional y alternativo
    - **d.** Número de teléfono.
    - **e.** Ubicación (edificio / nivel / oficina).
    - **f.** Diagrama del proyecto informático.
    - **g.** Nombre del lenguaje o *framework* de programación.
    - **h.** Nombre y versión de la base de datos (si aplicara).
    - **i.** Nombre y versión del *webserver* (si aplicara).

# 12. ANEXO B

## Código malicioso y ataques informáticos

1. En caso de notificación externa, interna o por inspección directa se encontrara código malicioso se tomará la siguiente línea de acción:

    a. *Ransomware*: se eliminará inmediatamente el recurso e informará a la UoD vía el responsable asignado. El proceso de restauración queda a discreción por el alto riesgo que conlleva trabajar con *ransomware* para toda la InfraDPD.
    b. El DPD notificará del incidente a la UoD para ofrecer un recurso recién instalado para que responsable de la UoD restaure su backup fuera de línea para la reconstrucción completa.
    c. *Phishing* inserto, se procederá a eliminar si fuera posible, donde esté alojado e informará a la UoD vía el responsable asignado.
    d. Contenido ilegal o no alineado con los fines de la Universidad de cualquier tipo: se hará una copia para análisis forense en frío y se eliminará inmediatamente el recurso e informará a la UoD vía el responsable asignado.

2. En caso de ser víctima la UoD que usa recursos de InfraDPD de ataques DDoS, *plugins* maliciosos o de explotación de alguna vulnerabilidad reportada en https://www.cvedetails.com el responsable debe notificar al DPD de esta situación para trabajar en conjunto la estrategia de defensa.

3. Casos desconocidos o en curso de identificación serán tratados en conjunto con el responsable de la UoD.



Sótano Edificio de Rectoría, Ciudad Universitaria Zona 12, Guatemala, Guatemala.
+502 2418-9651 dpdcorres@usac.edu.gt www.dpd.usac.edu.gt