

EMPRESA DISTRIBUIDORA ELECTRICA SALVADOREÑA
MANUAL DE POLÍTICAS -POLÍTICAS INFORMÁTICAS

Código de Política: PIT-09-PAS-A10-2018
POLÍTICA DE ANTIVIRUS Y SPAM (PAS)

- **Consideraciones generales**

1. Esta política está desarrollada para proteger las comunicaciones y sistemas informáticos de EDESAL, S.A. de C.V. frente a virus y otro software malicioso (SPAM o Malware).
2. El alcance de esta política se circunscribe a todos los equipos informáticos de EDESAL, S.A. de C.V. que se conecten a las redes corporativas y de datos de cada sucursal comercial.
3. Los equipos integrados en la red de datos de EDESAL, S.A. de C.V. tienen instalado un antivirus corporativo gestionado centralizadamente y que se actualiza automáticamente de forma periódica. Este antivirus es administrado exclusivamente por el Departamento de Informática.
4. Todos los ordenadores deben ejecutar una versión actualizada de un software antivirus. Este software debe ser capaz de proteger al sistema operativo en tiempo real y de actualizarse de forma automática cada vez que se conecte a la red de datos de EDESAL, S.A. de C.V.
5. Mientras el sistema esté conectado a la red no se debe detener, en ningún caso, la protección y actualización del antivirus.
6. Cuando se sospeche de una infección o cuando el antivirus detecte una, se debe desconectar el equipo de la red y proceder a su limpieza. En caso de no poder realizarse esta limpieza se debe contactar al Departamento de Informática. En caso de que el virus comienza a ocasionar daños en el sistema se debe apagar el ordenador de inmediato.

7. En ningún caso, incluido cualquier fin laboral, los usuarios pueden escribir, compilar, copiar, propagar o ejecutar de forma intencionada en equipos que se conecten a la red de datos un código diseñado para replicarse, dañar, espiar o entorpecer el desempeño de cualquier sistema de EDESAL, S.A. de C.V.
8. El sistema antivirus se encarga de escanear todos los correos (evitar SPAM) de ingreso a EDESAL, S.A. de C.V. a buzones institucionales con el fin de garantizar la proveniencia y seguridad de la información recibida.

- ***Incumplimiento***

9. El incumplimiento de esta política puede acarrear la revocación de privilegios de acceso o el bloqueo de comunicaciones y su reincidencia en casos de ser demostrable por parte de un empleado o contratista puede llevar a una sanción administrativa.