EMPRESA DISTRIBUIDORA ELECTRICA SALVADOREÑA
MANUAL DE POLÍTICAS -POLÍTICAS INFORMÁTICAS

POLÍTICA DE CONEXIONES REMOTAS (PCR)

- ***Consideraciones generales***

1. La política de conexiones remotas es extensiva para todos los empleados y contratistas de EDESAL, S.A. de C.V. que requieran y les sea autorizado el acceso a terminales o servidores institucionales a través de herramientas VPN para el desarrollo de sus actividades en horarios fuera de los normales o desde ubicaciones diferentes a las oficinas centrales en Ciudad Versailles o en la ubicación designada como principal para la ejecución de sus labores diarias.

- ***Responsabilidades del Departamento de Informática***

- Establecer e implementar los métodos de conexión remota a la plataforma tecnológica de EDESAL, S.A. de C.V.
- Implementar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica Institucional.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de EDESAL, S.A. de C.V. de manera permanente.

- ***Responsabilidades de los usuarios***

- Contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de EDESAL, S.A. de C.V. y deben acatar las condiciones de uso establecidas para dichas conexiones.

- Mantener en total reserva las direcciones de entrada a las direcciones Institucionales (direcciones ip o direcciones Web) al igual que las credenciales que les han sido otorgadas para su resguardo.
- Mantener la confidencialidad y protección de la información a la que tienen acceso fuera de las instalaciones Institucionales.
- Aplicar herramientas de antivirus sobre sus computadores personales, en lo posible, para brindar una mayor protección a los archivos e información que están gestionando.
- Dar aviso al Grupo de Soporte Tecnológico de cualquier posible abuso o intento de violación tanto de los accesos como de las credenciales entregadas.

- ***Monitoreo***

2. El Departamento de Informática, sin previo aviso, pueden realizar monitoreo para verificar el estado de las conexiones remotas, así como el tiempo y uso efectuado a través de este medio y efectuar las respectivas optimizaciones e informes.