EMPRESA DISTRIBUIDORA ELECTRICA SALVADOREÑA
MANUAL DE POLÍTICAS -POLÍTICAS INFORMÁTICAS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PITSI)

- ***Consideraciones generales***

1. EDESAL, S.A. de C.V. se compromete a salvaguardar la información que genera en la ejecución de sus operaciones institucionales, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, empleados y contratistas, y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión.
2. Toda la información que es generada por los empleados y contratistas de EDESAL, S.A. de C.V. en beneficio y desarrollo de las actividades propias de la empresa es propiedad del EDESAL, S.A. de C.V., a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a EDESAL, S.A. de C.V. de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Empresa.
   - EDESAL, S.A. de C.V. protege la información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta.
   - EDESAL, S.A. de C.V. protege su información de amenazas de sistemas o personas con malas intenciones.
   - EDESAL, S.A. de C.V. protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- EDESAL, S.A. de C.V. controla la operación de sus procesos de operación garantizando la seguridad de los recursos tecnológicos, redes y bases de datos.
- EDESAL, S.A. de C.V. implementa control de acceso a la información, aplicativos, recursos de red, portales y sistemas de información internos y externos o con accesos remotos.
- EDESAL, S.A. de C.V. garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- EDESAL, S.A. de C.V. garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- EDESAL, S.A. de C.V. garantiza la disponibilidad de sus procesos de operación y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Las responsabilidades frente a la seguridad de la información de EDESAL, S.A. de C.V. son definidas, compartidas, publicadas por la administración de la empresa y deberán ser aceptadas por cada uno de los empleados y contratistas de la Empresa.

- ***Responsabilidades del Departamento de Informática frente a la Seguridad de la Información.***

3. Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información, el uso de los servicios tecnológicos en toda la empresa de acuerdo a las mejores prácticas y lineamientos de la Gerencia General.
4. Mantener la custodia de la información que se almacena en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
5. Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Empresa a la

Gerencia General, las diferentes dependencias y Jefaturas de EDESAL, S.A. de C.V.

6. Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
7. Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de EDESAL, S.A. de C.V.
8. Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en EDESAL, S.A. de C.V.
9. Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Gerencia General (dicha habilitación puede ser de carácter temporal o definitiva dependiendo de la opinión y justificación presentado a la Gerencia General).
10. Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.
11. Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes dependencias y Jefaturas.
12. Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
13. Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la Empresa.

- ***Responsabilidades de los Empleados y Contratistas frente a la Seguridad de la Información.***

14. Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas ya sea en su perfil de puesto o en funciones especiales designadas por la administración de EDESAL, de acuerdo con los permisos establecidos o aprobados en el área de desempeño de sus labores.
15. Manejar la Información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
16. Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
17. Evitar la divulgación no autorizada o el uso indebido de la información.
18. Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
19. Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
20. Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
21. Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos o información que identifique.
22. Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico-científicos designados para el desarrollo de sus funciones.
23. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a EDESAL, S.A. de C.V. (salvo mediante previa autorización con la Gerencia General y el Departamento de

Informática) a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por el Departamento de Informática.

24. Usar software autorizado que haya sido adquirido legalmente por la Institución.
25. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno del Departamento de Informática.
26. Divulgar, aplicar y el cumplir con la presente Política.
27. Aceptar y reconocer que en cualquier momento y sin previo aviso, la administración, puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web visitados y enlace con las redes sociales, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Empresa. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
28. Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Empresa.
29. EDESAL, S.A. de C.V. no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves cuando lo realice de carácter personal con los activos tecnológicos e información propiedad de EDESAL, S.A. de C.V.

- ***Seguridad Lógica de la Red de Datos.***

30. El Departamento de Informática no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
31. Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
32. No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de Las Empresas.
33. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de EDESAL, S.A. de C.V. y se usarán exclusivamente para actividades relacionadas con la labor asignada.
34. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
35. Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

- ***Seguridad Perimetral***

36. El Departamento de Informática implementará soluciones lógicas y físicas que garanticen la protección de la información de EDESAL, S.A. de C.V. de posibles ataques internos o externos. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.
    - Rechazar conexiones a servicios comprometidos.
    - Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
    - Proporcionar un único punto de interconexión con el exterior.

- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

- ***Firewall***

37. La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores. Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
38. El Departamento de Informática establecerá las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
    - El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
    - El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
    - Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

- ***Redes Privadas Virtuales (VPN)***

39. Los usuarios móviles y remotos de EDESAL, S.A. de C.V. podrán tener acceso al a red interna privada cuando se encuentren fuera de La Empresa alrededor del mundo en cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por el Departamento de Informática.
40. Personal del Departamento de Informática será el encargado de configurar el software necesario y asignar las claves a los usuarios que lo soliciten a través de una solicitud del Jefe Inmediato o Gerente de área del solicitante registrando su respectivo Ticket en el sistema Comanda.