*

POLITICAS

1.1. POLITICA DE ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION

"SEDAPAL define roles, responsabilidades y segregación de funciones respecto a la seguridad de la información; asimismo, mantiene contactos apropiados con las autoridades relevantes y grupos especiales de interés; y toma en cuenta la seguridad de la información en la gestión de proyectos; y establece la política para el uso de dispositivos móviles y teletrabajo".

Política de dispositivos móviles

"SEDAPAL establece una política de dispositivos móviles con la finalidad de asegura que la información de la empresa no se comprometa cuando se usen dispositivos de informática móvil como Laptops, Tablets y Smartphone, estableciendo lineamientos que nos permitan tener un correcto uso de los mismos".

Política de teletrabajo

"SEDAPAL establece una política de teletrabajo con la finalidad de asegurar mediante lineamientos el ingreso a la red corporativa, protegiendo de esta manera la información de la empresa".

1.2. POLITICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

"SEDAPAL realiza la verificación de antecedentes de los candidatos al empleo, acorde con las leyes, regulaciones, ética y en proporción a: los requisitos del negocio, la clasificación de la información y los riesgos percibidos; asimismo, incluye acuerdos de confidencialidad para preservar la seguridad de la información, los cuales deben estar debidamente firmados por los trabajadores.

SEDAPAL solicita a todos los trabajadores y servicios tercerizados la aplicación de la seguridad de la información en sus actividades diarias, de acuerdo a las políticas y procedimientos establecidos; brinda una adecuada concientización, educación y capacitación; asimismo, establece procesos disciplinarios a los trabajadores y servicios tercerizados que hayan generado algún incidente de seguridad de la información; proteger los activos de información después de la desvinculación o cambio de relación laboral.
SEDAPAL requiere que en la desvinculación laboral, el trabajador se compromete a devolver todo activo y mantener por tiempo indefinido la confidencialidad de la información que tuvo acceso."

1.3. POLITICA DE GESTION DE ACTIVOS

"SEDAPAL establece la identificación de los activos de información; mantiene un inventario actualizado; y asigna los propietarios correspondientes. Asimismo, identifica, documenta e implementa las reglas para el uso aceptable de los activos de información; y en la finalización de la relación laboral determina la devolución de los activos de información de SEDAPAL asignados a los trabajadores.
SEDAPAL establece la clasificación de la información, de acuerdo a los requisitos legales, criticidad y sensibilidad a la divulgación o modificación no autorizada:

- *Público: Información no sensible de acceso público y que su divulgación no genere impacto en la organización*

- *Uso Interno: Activo de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la organización*
- *Confidencial: Activo de información cuyo contenido no debe ser divulgado ni distribuido a personas que no son autorizadas; y cuya difusión genere impacto en la organización*

Los activos de información se etiquetan de acuerdo al esquema de clasificación adoptado por SEDAPAL, esto incluye información impresa y digital.

SEDAPAL previene la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios, mediante procedimientos para la gestión de los medios removibles, eliminación de los medios de forma segura y protección de los medios durante su transporte."

1.4. POLITICA DE CONTROL DE ACCESO

"SEDAPAL establece procedimientos documentados para asegurar el acceso de usuarios autorizados a los sistemas, servicios y redes; establece el registro y baja de usuarios, la asignación y revocación de accesos; restringe y controla los accesos privilegiados; gestiona las contraseñas de accesos; revisa los derechos de acceso periódicamente; y asegura las remoción de accesos al termino del empleo. Establece el cumplimiento de las disposiciones establecidas para el uso de las contraseñas, debiendo ser éstas de calidad. Restringe y controla el uso de herramientas informáticas privilegiadas y el acceso a los códigos fuentes de los programas."

1.5. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

"SEDAPAL define los perímetros de seguridad físicas de las áreas seguras (áreas que contienen información sensible e instalaciones de procesamiento de la información); asegura el acceso físico no autorizado; aplica la protección física contra amenazas externas y ambientales; aplica controles de acceso y asilamiento a las áreas de despacho y carga.

SEDAPAL previene la pérdida, daño, robo o actos que comprometan los activos de información y la interrupción de las operaciones, mediante: la ubicación y protección adecuada de los equipos ante las amenazas ambientales; la protección contra fallas del suministro de los servicios (energía eléctrica, aire acondicionado, entre otros), la protección ante interceptación, interferencia o daño del cableado de energía y datos; el mantenimiento de equipos; el retiro debidamente autorizado de los equipos, software e información; la aplicación de seguridad de equipos y activos fuera de las instalaciones; la eliminación o reutilización segura de los equipos; y el establecimiento de política de escritorio limpio y pantalla limpia".

Política de escritorio y pantalla limpia

"SEDAPAL establece mediante una política de escritorio limpio para reducir el riesgo de accesos no autorizados, pérdida o daño a la información impresa expuesta en los escritorios y una política de pantalla limpia con el fin de proteger la información almacenada en el computador mediante el establecimiento de mecanismos de bloqueo para las estaciones de trabajo cuando estos estén inactivos por un tiempo determinado; durante el horario normal de trabajo como fuera del mismo".

1.6. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

"SEDAPAL documenta sus procedimientos, instructivos, manuales, formularios y otros documentos, manteniendo un control sobre los cambios en la organización, el negocio y los sistemas; asegura el desempeño de los recursos; mantiene la separación de los ambientes de desarrollo, calidad y producción; adopta las medidas necesarias para la prevención, detección y eliminación de software malicioso; protege la información contra pérdidas mediante copias de

respaldo de la información; registra y monitorea los eventos de seguridad de la información; establece controles en la instalación de los sistemas de información; gestiona las vulnerabilidades técnicas de los sistemas de información; establece e implementa restricciones respecto a la instalación de software; minimiza las interrupciones de los procesos del negocio durante las auditorías de los sistemas de información".

1.7. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

"SEDAPAL protege la información en las redes, por medio de: la gestión y control de las redes, seguridad en los servicios de red, y la separación de las redes. Mantiene la seguridad en la transferencia de la información internamente y con cualquier entidad externa, por medio de: políticas y procedimientos, acuerdos de transferencia segura de información entre la organización y terceros; acuerdos de confidencialidad o acuerdos de no divulgación; y el uso de mensajería electrónica segura".

1.8. POLITICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

"SEDAPAL establece que los requisitos de seguridad de la información es parte de los requisitos de los sistemas de la información nuevos o existentes; asegura los servicios de aplicación en redes públicas; y protege las transacciones de los servicios de aplicación.
SEDAPAL establece la seguridad de la información dentro del ciclo de desarrollo de los sistemas de información implementando: reglas para el desarrollo de software seguro; procedimientos de control de cambios del sistema; revisión y pruebas de las aplicaciones críticas; restricciones en los cambios en los paquetes de software; principios de ingeniería de sistemas seguros; entornos de desarrollo seguro; supervisión y monitoreo de los desarrollos de sistemas tercerizados; pruebas de seguridad del sistema; pruebas de aceptación del sistema. Asimismo, asegura la protección de los datos utilizados durante la fase de pruebas".

1.9. POLITICA DE GESTIÓN DE ENTREGA DE SERVICIOS DEL PROVEEDOR

"SEDAPAL asegura la protección de sus activos de información que son accesibles por los proveedores, estableciendo la política para las relaciones con los proveedores, definiendo la seguridad dentro de los acuerdos del proveedor, acordando y documentando con el proveedor los requisitos de seguridad de la información de los servicios.
SEDAPAL mantiene un nivel de seguridad de la información en la entrega de servicios por parte de los proveedores, supervisando y revisando los servicios del proveedor, y gestionando los cambios en los servicios del proveedor".

1.10. POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

"SEDAPAL implementa una gestión de incidentes de seguridad de la información, así como la comunicación de los eventos de seguridad y debilidades, estableciendo responsabilidades y procedimientos, informando los eventos y debilidades de seguridad de la información mediante canales apropiados, evaluando los eventos de seguridad de la información, dando respuesta a los incidentes de seguridad de la información de acuerdo a procedimientos documentados, utilizando el conocimiento adquirido y definiendo y aplicando procedimientos para la recolección de evidencias".

1.11. POLITICA DE LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

"SEDAPAL incorpora la continuidad de la seguridad de la información en su sistema de gestión de continuidad del negocio, planificando, implementando y evaluando la continuidad de la seguridad de la información".

1.12. POLITICA DE CUMPLIMIENTO

"SEDAPAL cumple con las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad, identificando la legislación vigente y los requisitos contractuales; implementando procedimientos apropiados para el cumplimiento de los derechos de propiedad intelectual y uso de software patentados; protegiendo los registros; asegurando la privacidad y protección de la información de identificación personal; y utilizando controles criptográficos según regulación pertinente.
SEDAPAL garantiza que la seguridad de la información sea implementada y operada de acuerdo a sus políticas y procedimientos, efectuando revisiones independientes de la seguridad de la información y cumplimiento de las políticas y normas; y verificando de manera regular el cumplimiento de las políticas y normas de seguridad de la información".