Política de Seguridad de la Información

Objetivos Seguridad de la Información

Garantizar la disponibilidad de los servicios críticos acordados con los clientes internos y externos

Desarrollar una cultura consciente de la importancia de la seguridad de la información

Promover el cumplimiento de los requisitos legales, reglamentarios y contractuales en materia de seguridad

- Control de acceso áreas e información
- Uso de claves y contraseñas
- Uso del correo electrónico
- Uso de internet
- Requisitos de seguridad para estaciones de trabajo
- Requisitos de seguridad para equipos móviles
- Equipo desatendido
- Uso de medios de almacenamiento
- Protección de datos y confidencialidad

TRIADA DE SEGURIDAD DE LA INFORMACIÓN

Confidencialidad

•Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad

•Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad.

Integridad

•Propiedad de la información relativa a su exactitud y completitud.

Objetivo del Sistema de Gestión Seguridad de la Información

Establecer los mecanismos y herramientas de gestión que permitan la disponibilidad, confidencialidad e integridad de los activos de información.

Políticas de Seguridad de la Información

Generar atributos de confidencialidad de la información en actividades y procesos.

Proteger la integridad de la información en los procesos del negocio.

Establecer mecanismos de disponibilidad de la información y los sistemas y servicios de tecnología de la información

Cumplir la legislación actual aplicable al ejercicio.

Políticas para dispositivos móviles

•No está permitida la movilización de equipos con información clasificada como confidencial.

•No es aceptada la conexión a redes públicas desde equipos de DOMINA o con información sensible bajo la responsabilidad de la empresa.

Políticas Transferencia de Medios Físicos

- Los medios de almacenamiento como memorias USB, CD, DVD y demás unidades de este tipo, son de uso restringido.
- Los puertos y unidades de lectura están bloqueados para evitar fuga de información.

Política de controles criptográficos

CIFRADO

•La información que por petición del cliente deba ser codificada, será tratada por medio de la política de encriptación.

AUTORIZACIÓN

•Solo al personal autorizado se le permite codificar y decodificar la información.

Política de Seguridad Física

•CÁMARAS

•Las instalaciones cuentan con circuito cerrado de información.

•CARNÉ

•El personal debe de estar identificado con carné mientras está en las instalaciones.

•VISITANTES

•Los visitantes deben ser registrados, identificados y definidas las áreas a las que tendrá acceso.

Política de Controles Código Malicioso

INFORMAR

Es deber de todos los usuarios reportar código malicioso en caso que se den cuenta de ello.

ELIMINAR

Los mensajes de correo electrónico identificados como peligroso, deben ser eliminados en el mismo momento que sean identificados.

Política de Transferencia de Información

TRANSFERENCIA

La transferencia de información clasificada como confidencial debe ser a través de medios seguros.

CIFRADO

La información sensible como bases de datos debe ser transmitida de manera cifrada.

MEDIOS

Para la trasferencia de información se debe utilizar el correo corporativo.

Política de Relaciones con Proveedores

DOMINA define claramente la política de relación con los proveedores a través de:

•Requisitos técnicos relacionados con la seguridad de la información
•Autorización y entrega de información adicional
•Acceso físico a los activos de información y equipos tecnológicos
•Acceso remoto a través de herramientas informáticas (únicamente como SFTP o Red Privada Virtual VPN, cuando ello sea necesario para el cumplimiento de la ANS o el contrato)
•Contratación de servicios tecnológicos
•Seguridad en la instalación y configuración de activos tecnológicos
•Inspección y auditoría de las condiciones del servicio.

Política de Relaciones con Proveedores

- Acuerdos de custodia y confidencialidad de la información
- Seguridad en el intercambio de información con proveedores
- Requisitos de certificación de seguridad de los proveedores
- Manejo de incidentes de seguridad asociados a los servicios
- Acuerdos de niveles de servicios y los planes de recuperación
- Monitoreo y seguimiento sobre los servicios tecnológicos externalizados
- Entrega y difusión de las políticas de seguridad a proveedores.

DATO PERSONAL

Conjunto organizado de datos personales que sea objeto de tratamiento

TITULAR

Personal natural cuyos datos personales sean objetivo de tratamiento

ENCARGADO

Es quien realiza el tratamiento de datos personales por cuenta del responsable del tratamiento

RESPONSABLE

Es quien recibe los datos personales y autorización del titular para hacer tratamiento y puede decidir sobre ellos.

Política de Protección de Datos Personales

En esta política se establecen los parámetros y procedimientos que reglamentan el tratamiento y protección de la información y datos personales, teniendo en cuenta su origen, mantenimiento, administración y demás operaciones que involucren manejo de la misma.
Para tales efectos, Domina se sujeta a las disposiciones reguladas en la ley y en la Constitución Política de 1991, en las cuales se consagra, reconoce y protege el derecho a la protección de datos personales como precepto que poseen todos los ciudadanos a conocer y actualizar información que haya sido recogida en bases de datos que sean susceptibles de tratamiento por parte de entidades de carácter público o privado.

La Seguridad de la Información es un compromiso de todos y por eso queremos contar contigo.

¡Gracias!


Domina
ENTREGA TOTAL