VINALI GROUP

POLÍTICAS Y PROCEDIMIENTOS

SGSI



ORGANIZACIÓN CERTIFICADA
Seguridad de la Información
ISO/IEC 27001

PROCEDIMIENTO DE CONTROL DE ACCESO

Vinali le entregará credenciales de acceso a plataformas y cuentas de acuerdo a las funciones que vaya a realizar.

Es su responsabilidad como funcionario mantener la confidencialidad e integridad de la información suministrada.



POLÍTICA DE TELETRABAJO

01

El personal que se encuentre autorizado para ejecutar sus funciones de forma remota debe informar de inmediato cualquier incidente de seguridad que se presente así como mantener comunicación con su jefe directo.

02

Los trabajadores y colaboradores que cuenten con equipo de cómputo brindado por la compañía deben limitar su uso a las funciones asignadas al cargo, de la misma forma deben promover la seguridad del activo.

03

El trabajador o colaborador debe usar los servicios de Wi-Fi provistos (referente a auxilios de conectividad) o seguros, se prohibe el acceso a redes Wi-Fi públicas.

POLÍTICA DE SEGURIDAD FÍSICA

Zonas Restringidas

Prohibido el acceso de cualquier persona que no cuente con la autorización expresa de hacerlo:

- Oficinas de gerencia y dirección: El funcionario responsable de estas debe aplicar mecanismos de control necesarios para prevenir el acceso no autorizado.

- Cuarto de equipos y Rack Room: El administrador de infraestructura está encargado de aplicar controles necesarios para prevenir el acceso no autorizado.

Acceso a Instalaciones Físicas

El acceso a las instalaciones debe ser previamente validado, todo funcionario autorizado tiene la responsabilidad de promover y controlar el buen uso de los dispositivos de ingreso.



USO DE ACTIVOS DE INFORMACIÓN

1. En cuanto al uso de impresoras, el usuario debe recopilar la impresiones de inmediato.

2. Para la información que se encuentre en tableros u otro tipo de pantallas, debe ser borrada en cuanto no se necesite.

3. Especialmente durante presentaciones, pantallas compartidas o en áreas públicas, se deben establecer reglas de configuración o reglas para ventanas emergentes.



ESCRITORIO Y PANTALLAS LIMPIOS

- Esta política es aplicable para todo tipo de información que se encuentre en escritorios, áreas de trabajo, equipos de cómputo, documentos en papel, medios de almacenamiento y en general cualquier tipo de información que usen los empleados.

- En cuanto a las piezas de información crítica que se encuentren en físico, se deben guardar preferiblemente bajo llave cuando no sea necesario, especialmente cuando se ausente de su puesto de trabajo.





GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Es responsabilidad de todo funcionario, empleado y/o colaborador informar inmediatamente al oficial de seguridad de la información sobre cualquier incidente de de seguridad de la información, los incidentes de información se catalogan como se evidencia a continuación:

- Fuga de información.
- Acceso no autorizado.
- Denegación de servicio.
- Fraudes, chantajes y/o amenzas.
- Contaminación por malware.
- Monitoreo de red.
- Suplantación de identidad.





POLÍTICA DE NAVEGACIÓN WEB SEGURA Y USO ADECUADO DE HERRAMIENTAS TECNOLÓGICAS

Las herramientas deben ser empleadas de forma adecuada y únicamente para fines laborales, se prohíbe de manera expresa el acceso a sitios web que no sean relacionados con las funciones propias de cada cargo.

Está prohibido visitar, entre otras:

- Visualización de contenido multimedia (películas y/o series).
- Páginas de apuestas.
- Contenido para adultos.

Es importante resaltar que cualquier conducta que vaya en sentido contrario de estos lineamientos será considerada como una falta y, por ende, estará sujeta a la acción disciplinaria correspondiente por parte del área de Recursos Humanos.

GRACIAS POR SU ATENCIÓN

Si tiene dudas puede siempre remitirse al "Manual de Políticas y Procedimientos SGSI" enviado previamente y/o puede consultar con nosotros.

Andrés Soto Sarmiento
Oficial de Seguridad de la Información
asoto@vinaligroup.com

Equipo de IT
itvinali@vinaligroup.com

VINALI GROUP