OBJETIVO

Dar a conocer las políticas y lineamientos del Sistema de Gestión de Seguridad de la Información necesarios para implementar los controles establecidos en el Anexo A de la NTP ISO/IEC 27001, los cuales permiten alcanzar los objetivos definidos para la seguridad de la información en la empresa.

ALCANCE

Aplica a todos las áreas, colaboradores y terceros relevantes que formen parte o brinden servicios a la empresa.

POLÍTICA DE DISPOSITIVOS MÓVILES

- Las características en las capacidades de los equipos deberán ser definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utiliza un dispositivo móvil de la organización.
- Todos los usuarios de dispositivos móviles que contengan información confidencial o de uso interno deben usar la última o la más segura versión de los productos de software. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.
- Se debe mantener actualizado el software antivirus de los dispositivos móviles.

POLÍTICA PARA EL USO ACEPTABLE DE LOS ACTIVOS

- El uso de la información y de los activos de información debe ser para propósitos de las actividades de la empresa de acuerdo a las políticas, procedimientos o cualquier lineamiento que definan.
- No se debe divulgar información que haya sido clasificada como confidencial o restringida, salvo autorización del propietario de información quien debe ser responsable de la divulgación.
- Cualquier acceso, modificación o eliminación de información o de un activo de información debe ser expresamente autorizada por el propietario de información o propietario del activo de información.
- Se deben cumplir con lo establecido en los requisitos legales, contractuales y normativos relativos al uso de activos de información.
- El personal que ponga en riesgo los activos de información, se le aplicará medidas disciplinarias de acuerdo al proceso disciplinario vigente.
- Todos los activos a los que tenga acceso un personal se encuentran bajo su responsabilidad y deben de proteger su integridad y confidencialidad.

Elaborado por:	Revisado por:	Homologado por:	Aprobado por:
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información**	Jorge Herbozo – **Líder de Gobierno Digital**	**Departamento de Planeamiento y Control de Gestión**	Juan Carlos Febres Teves - **Gerente General**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korel FAU 20425809882 hard Fecha: 09/06/2021 16:22:40	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 09/06/2021 11:51:51	**Firma:**	**Firma:** Firmado digitalmente por: FEBRES TEVES Juan Carlos FAU 20425809882 hard Fecha: 09/06/2021 18:58:34

Una vez impreso, compartido o descargado este documento se convierte en **copia no controlada** y una vez concluido su uso estos deberán ser eliminados**.** Verificar su vigencia en el repositorio.

- Todo activo que contiene información no debe ser desatendido, debe quedar resguardado bajo llave o se deben utilizar bloqueos especiales para asegurarlo.
- Todo incidente de seguridad de la información que involucre a información confidencial o a los activos que soportan dicha información deben ser reportados por los canales establecidos.

POLÍTICA PARA LA GESTIÓN DE MEDIOS REMOVIBLES

Se ha establecido la siguiente política específica para el uso de medios removibles que contienen información clasificada como “confidencial” o “restringida”:

- Los usuarios que usen medios removibles como memorias USB, discos externos, DVDs y CDs deben evitar utilizarlos en equipos internos o externos que no cuenten con las medidas de seguridad mínimas requeridas como un antivirus y de ser necesario solicitar al departamento de Tecnología de Información y Comunicaciones la implementación de controles de cifrado. Además, son responsables del aseguramiento físico de estos, en tal sentido, cuando no se estén usando deben quedar resguardados en un cajón con llave u otro espacio seguro.
- Los medios removibles no deben quedarse conectados en equipos desatendidos por largos períodos de tiempo.
- Los medios removibles deben ser devueltos por cese o cambio de posición de personal, y se debe realizar el borrado seguro de la información contenida en el medio.

POLÍTICA DE CONTROL DE ACCESOS

- El control de acceso a los sistemas de información debe realizarse por medio de códigos de identificación y contraseñas únicos para cada usuario. Las cuentas de usuario deben ser únicas para cada empleado y éste será responsable por toda actividad que sea realizada con dicho usuario.
- Se establece que el uso de contraseñas robustas debe estar configurado en los sistemas de información.
- Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro empleado.
- El nivel de acceso a un sistema de información se otorgará de acuerdo a:
  - La clasificación de la Información.
  - Funciones del usuario.
  - Perfiles de acceso estandarizados.
  - Pedido, autorización y administración de acceso.
  - Revisión periódica.
  - Retiro y modificación de derechos de acceso.
- Los sistemas de información, según su criticidad y uso, deberían desconectar automáticamente las sesiones de conexión tras un periodo definido de inactividad que sea configurable por cada sistema.

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo a la identificación previa de requerimientos de la organización y de seguridad de la información.
- Todos y cada uno de los equipos de cómputo deben ser asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
- Los accesos con altos privilegios (usuarios administradores) deben ser controlados igualmente mediante un procedimiento formal.
- Periódicamente se debe revisar que los accesos de las cuentas de usuario de personal cesado hayan sido eliminados y/o deshabilitados.
- Periódicamente se debe revisar que los accesos concedidos a los usuarios sean los que les corresponde de acuerdo a las funciones que desempeñan.
- El acceso a repositorios con código fuente debe ser controlado.

POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

- Se deberán utilizar controles criptográficos en los siguientes casos:
  - Para el uso de firmas digitales y certificados digitales.
  - Para el resguardo de información, cuando así resulte de la evaluación de riesgos realizada por el Propietario de Activo de Información o Propietario del Riesgo.

POLÍTICA DE EQUIPOS DE USUARIO DESATENDIDOS

- Al dejar un equipo desatendido temporalmente, el usuario debe bloquear el acceso a su computador, laptop o servidores, independientemente del tiempo que permanezcan alejados.
- Las estaciones de trabajo y terminales no deben estar activas cuando sean desatendidas y deben ser protegidas mediante uso de contraseñas u otros controles cuando no estén siendo utilizadas.
- Se debe establecer un método de bloqueo (contraseñas, patrones, etc.) para los equipos que serán entregados a los usuarios, y que se bloquee pasado un tiempo no mayor a cinco minutos de inactividad.
- Al terminar la jornada de trabajo se deberá apagar el equipo, siempre y cuando no se encuentren ejecutándose procesos programados fuera de horario de oficina y respondan a labores propias del cargo del trabajador. En caso de ausentarse de la oficina por un período prolongado de tiempo, se deberán cancelar las sesiones de usuario dentro de las aplicaciones, además de bloquear la pantalla.
- Todo usuario debe desconectarse de las aplicaciones o de servicios de red cuando ya no sea necesario.

POLÍTICA DE ESCRITORIO LIMPIO

- Es responsabilidad de todo colaborador mantener sus escritorios o puestos de trabajo limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio para evitar el acceso no autorizado o fuga de información.
- Se debe evitar exponer información confidencial e interna en los módulos, escritorios o estaciones de trabajo de la empresa.
- El colaborador o proveedor no deberá tener escrito en un medio físico (papel adhesivo, papel convencional, superficies, etc.) su cuenta de red, credenciales de acceso de correo electrónico, aplicación, sistema de información, datos personales o información relevante que comprometa la seguridad de la información.
- Al ausentarse del puesto de trabajo se deberá guardar en un lugar seguro información física o medios removibles que contengan información confidencial o sensible.
- Los documentos digitales enviados a impresión, se deberá recoger inmediatamente, toda vez que esta sea considerada como confidencial o sensible.
- No se arrojará al tacho de basura, documentos impresos que contengan información confidencial o sensible. Antes deben ser destruidos de forma irrecuperable.

POLÍTICA DE PANTALLA LIMPIA

- No se deberá almacenar en la pantalla del escritorio de la estación de trabajo, información digital conteniendo credenciales personales o corporativas o información confidencial que pueda comprometer la seguridad de la información.
- Se deberá mantener el escritorio del sistema operativo libre de archivos o iconos que saturen y confieran una práctica de almacenamiento riesgosa.
- Los archivos que contengan información confidencial o sensible deben ser guardados en un repositorio de red que cuente con seguridad de acceso y respaldo.

POLITICA DE TELETRABAJO / TRABAJO REMOTO

- Todas las políticas presentes son aplicables en trabajo remoto.
- El colaborador debe establecer un ambiente de trabajo adecuado para el desarrollo de sus actividades (considerar ergonomía, iluminación, entre otros).
- En la medida de lo posible, configurar el router con una contraseña segura.
- Resguardar en cajones o gavetas con llave los documentos físicos y medios de almacenamiento que contengan información clasificada como confidencial o restringida.
- En la medida de lo posible, evitar que personas no autorizadas accedan a tu estación de trabajo.

INCUMPLIMIENTO DE LAS POLITÍCAS

El incumplimiento de estas políticas de seguridad de la información traerá consigo las consecuencias legales que apliquen a la normativa y proceso disciplinario de la empresa.

Elaborado por:	**Revisado por:**	**Homologado por:**	**Aprobado por:**
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información**	Jorge Herbozo – **Líder de Gobierno Digital**	**Departamento de Planeamiento y Control de Gestión**	Juan Carlos Febres Teves - **Gerente General**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korel FAU 20425809882 hard Fecha: 09/06/2021 16:22:40	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 09/06/2021 11:51:51	**Firma:**	**Firma:** Firmado digitalmente por: FEBRES TEVES Juan Carlos FAU 20425809882 hard Fecha: 09/06/2021 18:58:34

Esta es una copia auténtica imprimible de un documento electrónico archivado por ADINELSA, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM, y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la lectura del código QR o el siguiente enlace:
https://tramite.adinelsa.com.pe/consulta/dlFile?var=t8GCyIKAg4%2B%2BvqCiYFeng2WiZ1JdtalgtXR6fnW8srGgoIXU

Una vez impreso, compartido o descargado este documento se convierte en **copia no controlada** y una vez concluido su uso estos deberán ser eliminados. Verificar su vigencia en el repositorio.