POLÍTICA DE SEGURIDAD INFORMÁTICA

OBJETIVO: Establecer los lineamientos, normas y parámetros para la administración del sistema de información de la organización.

GENERALIDADES:

1. El Jefe de Tecnología de la Información es quien gestiona y administra los recursos tecnológicos.
2. La asignación de usuario y contraseña, que es personal e intransferible es administrada por Tecnología de la Información de acuerdo con lo establecido en el procedimiento “Control al sistema de información”, la cual se debe cambiar cada 90 días para mitigar el riesgo de suplantación.
3. Para la creación y actualización de contraseñas se establecen parámetros mínimos, los cuales están descritos en el procedimiento “Control al sistema de información”.
4. Está prohibida la instalación de programas o aplicaciones por parte de los colaboradores de la organización. El proceso Tecnología de la Información es responsable de la instalación, actualización y/o desinstalación de programas informáticos alineados a las normas de protección de derechos de autor.
5. La navegación en Internet debe estar alineada con sus funciones y roles asignados. El acceso a páginas de ocio no productivas, como los son: redes sociales, páginas de streaming de video y de audio (Facebook, YouTube, Instagram, Emisoras, Proxy, entre otros) no está permitido.
6. Los datos, documentos, carpetas y registros generados por los usuarios, correspondientes a sus actividades laborales, son propiedad de la organización, por tanto, cualquier divulgación o copia a entes externos sin autorización de la organización se considera una violación a la confidencialidad de la información y una falta grave de acuerdo con el reglamento interno de trabajo.
7. Cada colaborador es responsable del equipo que se le asigna y la información que este almacene.
8. Toda la información producto de sus labores debe almacenarse en la carpeta con nombre “OneDrive – MIEMPRESA”, en dicha carpeta se asegura la custodia, integridad y disponibilidad de la información, en caso de no tener la carpeta disponible se debe reportar inmediatamente al proceso de Tecnología de la Información.
9. Las únicas herramientas autorizadas para almacenamiento de información corporativa en la Nube son las descritas y autorizadas en el procedimiento
10. El uso de herramientas para almacenamiento de información en la nube como OneDrive o SharePoint debe ser exclusivo para procesos o documentos propios de sus funciones.
11. Se prohíbe a los colaboradores acceder, manipular o descargar, archivos de SharePoint o OneDrive en equipos que no sean propiedad de la organización.

12. El uso compartido de documentos en herramientas como SharePoint y OneDrive debe realizarse únicamente entre colaboradores de la organización, utilizando exclusivamente las cuentas de correo corporativas asignadas por personal de TI.
13. Es responsabilidad del usuario conocer la naturaleza de los documentos que se comparten a través de herramientas de almacenamiento en la Nube como OneDrive y SharePoint con otros colaboradores, entendiendo el principio de confidencialidad e integridad de los datos.
14. Los sistemas de información establecidos para el manejo, recepción y envío de información son los definidos en el proceso “Control al sistema de información”.
15. El almacenamiento en medios externos como lo son: USB, UNIDADES QUEMADORAS, CINTAS MAGNETICAS, entre otros, está restringido, de acuerdo con la MATRIZ DE ROLES.
16. Se prohíbe el envío de información de la empresa desde o con destino a cuentas de correo o sistemas de almacenamiento personal de los colaboradores.
17. El acceso o intento de acceso violento a información a la cual no se le ha otorgado permisos de ingreso por parte de Tecnología de la Información se contempla como una violación a la confidencialidad de la información.
18. Los daños físicos ocasionados a recursos de tecnología, bien sea por uso inadecuado o abuso, deben ser directamente asumidos por la persona que tenga el equipo o activo asignado.
19. Está prohibido el consumo de alimentos y bebidas en los puestos de trabajo, ya que esto puede ocasionar daños involuntarios a los recursos tecnológicos.
20. En caso de robo o pérdida del equipo o activo, deberá presentarse denuncia a las autoridades competentes de manera inmediata. El valor de reposición de este debe ser asumido por la persona a quien se asigna, y el suceso debe ser reportado posteriormente a Tecnología de la Información, Capital Humano y Gestión Compras.
21. Es responsabilidad del usuario bloquear sesiones de trabajo una vez termine su jornada laboral o haga pausa de esta (ejemplo: hora de almuerzo o break).

SANCIONES: El incumplimiento de cualquiera de las condiciones establecidas en esta política acarreara directamente al infractor un proceso disciplinario según lo establecido en el Reglamento Interno de Trabajo.

Firma: Miguel Florez (Nov 30, 2020 20:54 EST)

Miguel Angel Florez Palacios

Gerente General