



POLÍTICA CONFIDENCIALIDAD DE LA INFORMACIÓN

CÓDIGO: GG-DC-24

VERSIÓN: 0

FECHA: 19/06/2024

Con el fin de garantizar la seguridad de los procesos realizados con la **INFORMACIÓN INSTITUCIONAL**, todo el personal de **SERVILIN LTDA**, debe adaptar los lineamientos dados por la Gerencia para el manejo COMPUTADORES, DESKTOP, LAPTOP, TERMINALES IP, SERVIDORES TERCERIZADOS, TELEFONOS. Esto con el fin de cumplir con el Principio CID de la información. (Confidencial, Integral y Disponible), enmarcado dentro del proceso y aplicando el Reglamento Interno de Trabajo.

- 1. Ordenamiento:** Cada usuario clasificará y organizará la información de su dependencia en carpetas alojadas en sus equipos asignados. Se aplicarán las técnicas de archivo y denominación para su correcto almacenamiento, ubicación y disponibilidad. La información será única y exclusivamente de la empresa.
- 2. Aseguramiento:** El usuario asume la responsabilidad de mantener copias de seguridad. Hará los respectivos cargues al servidor semanalmente o en tiempo real, o como se aplique mejor dentro de la operación diaria. Este criterio y ejercicio será revisado dentro del cronograma de mantenimiento de la información cada 6 meses por TIC.
- 3. Protección:** El usuario supervisará el funcionamiento y las notificaciones que genere el Antivirus o el Firewall, cada vez que reporte una alerta. Cada archivo procesado en su equipo y que sea de origen externo, será validado con estas herramientas evitando la penetración de SCRIPS, RANSOMWARE, VIRUS, TROYANOS Y/O MALWARES. Toda información tiene un dueño y diferentes niveles de sensibilización, Ley 1581 de 2012 (Habeas data). Por tal razón toda información procesada y/o encontrada dentro de los equipos de la empresa procede a ser de propiedad de la misma.
- 4. Concientización:** El usuario asume el compromiso de no exponer la información institucional con el descargue de juegos, programas, Apps, música, videos ni archivos que no corresponden a la gestión corporativa. Tampoco se visitará páginas de ocio, descargas, películas, clasificación para mayores, y/o páginas que generen cookies de notificación y phishing (emisoras, TV, algunas redes sociales, de compra de chat, de intercambio) sin la debida autorización y asesoría. El usuario advertirá el peligro de las ventanas emergentes y de ser el caso se consultará con TIC.
- 5. Acceso:** Su estación y/o puesto de trabajo siempre debe cumplir con: contraseña de inicio con parámetros WAP, Bloqueo de pantalla, No desinstalará ni modificará las directivas establecidas al momento de recibir su equipo. En caso de afectar los inventarios de licenciamiento, el usuario asumirá la responsabilidad civil y contractual. Si el equipo debe ser llevado



POLÍTICA CONFIDENCIALIDAD DE LA INFORMACIÓN

CÓDIGO: GG-DC-24

VERSIÓN: 0

FECHA: 19/06/2024

fuera de las instalaciones solicitara un permiso temporal o permanente con la gerencia para aplicar directivas avanzadas.

- 6. Supervisión:** El usuario asume TOTAL RESPONSABILIDAD de trafico de correo, incluyendo los spams, y/o correo no deseado. Toda infiltración depende de la supervisión y clasificación detallada. Esto evitara los RANSOMWARE, que son la amenaza más común. Todo correo que mencione POLICIA, DIAN, JUZGADO, DEMANDA, COMPARENDO O SANCIÓN, o similar, será revisado minuciosamente y con acompañamiento del área de TIC.
- 7. Contingencia:** El usuario se compromete seguir detalladamente estos principios fundamentales para la gestión de atención a cualquier CONTINGENCIA probable. En tal caso se apoyará con las copias de seguridad e igualmente con las máquinas de soporte.
- 8. Cuidados generales:** El usuario supervisara, las rendijas de ventilación estén libres y operativas, no brindara claves de uso personal institucional, no consumirá bebidas y alimentos que puedan contaminar físicamente su estación y/o puesto de trabajo. No manipulara cables eléctricos, ni cables de conexión de su terminal IP, computador o impresora. Si su equipo es portátil y necesita moverlo, ciérrelo temporalmente y luego si puede ser transportado. Dado que el equipo es para uso personal, la limpieza y orden corresponden al Usuario. Mientras este apagado, puede limpiarlo con un paño levemente húmedo o con aspersion de alcohol y un paño suave.
- 9. Encriptación:** Como usuarios involucrados en el manejo de Documentos Oficiales y confidenciales, nos comprometemos y adoptamos la práctica de proteger los documentos abiertos, aplicarles métodos de decodificación para consulta, encriptar transmisiones de correo y sus adjuntos.

DANCERI LÓPEZ JARAMILLO
REPRESENTANTE LEGAL
19/06/2024