POLÍTICA DE
USO ACEPTABLE DE LOS ACTIVOS

Versión	Revisión	Elaboró	Aprobó	Fecha
0002	0003	O.L.	R.C.	03/11/2023

Acerca de esta Política

El propósito de esta política es garantizar que todos los empleados conozcan y apliquen prácticas aceptables en el uso de los activos de información, asegurando que todos los activos de información sean clasificados, protegidos y gestionados.
Esta política está diseñada para definir las pautas y responsabilidades del usuario al usar y manipular la información, garantizando que está protegida y se use con fines legítimos, de modo que exista un compromiso total con seguridad de la información.

Alcance

Esta política es aplicable a todos los miembros del personal de la empresa.

Definiciones

- **Activo de la Información:** Es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.
- **Activos de TI:** Los activos de Tecnologías de la Información (TI) son componentes físicos o lógicos utilizados para capturar, almacenar, procesar o transmitir información en el entorno empresarial. Esto incluye, pero no se limita a, dispositivos como computadoras, servidores, dispositivos de red, dispositivos móviles, software, sistemas de almacenamiento y cualquier otro elemento tecnológico relacionado con la gestión y el procesamiento de información en la organización
- **Uso Aceptable:** Se refiere a las prácticas, políticas y directrices que regulan la utilización de los activos de la información dentro de una organización. Estas normas establecen los límites y las responsabilidades de los usuarios al interactuar con los activos de la información. El Uso Aceptable define las actividades permitidas y restringidas, garantiza la protección de la información confidencial y promueve un comportamiento ético y seguro por parte de los empleados y otros usuarios autorizados
- **Escritorio limpio:** Protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en estaciones de trabajo, de accesos no autorizados, perdida o daño de la información.
- **Estación de trabajo:** Área dispuesta por Loginter S.A. para que cada colaborador pueda llevar a cabo sus actividades. Tales como oficinas, escritorios entre otros.

- **Lugar seguro:** es aquel que protege el activo de información de acceso de personas no autorizadas, que su contenido no sea alterado y que el activo pueda ser recuperado por las personas autorizadas de manera oportuna (algunos ejemplos son: cajón seguro con llave, oficina con llave, etc.)
- **Pantalla limpia:** Protección de los equipos de cómputo, tabletas, portátiles u otros dispositivos mediante un bloqueo de pantalla o desconexión cuando no está en uso.

Documentación de referencia

Norma ISO 27001.

Uso aceptable de los activos de la Información

Uso aceptable

Los activos de la información solo se podrán utilizar para llevar a cabo actividades profesionales con el fin de realizar tareas relacionadas con Loginter.

Responsabilidad sobre los activos

Todos los activos de la información tendrán un propietario designado en el inventario de activos. El propietario del activo será responsable de la confidencialidad, integridad y disponibilidad de la información del activo.

Retiro de los activos físicos

Los activos de TI utilizados en el trabajo cotidiano, como dispositivos digitales y equipos relacionados, podrán ser retirados de su lugar de almacenamiento, siempre y cuando se realice la solicitud o procedimiento indicado y que sea correctamente identificado. La solicitud de retiro de activos físicos deberá ser realizada por el jefe del área responsable, formalizando la petición vía correo electrónico, sistema de tickets o en cumplimiento del procedimiento establecido.

Devolución de los activos

Ante la desvinculación laboral, todos los activos de la información de Loginter deberán ser devueltos por el colaborador, en cumplimiento con los procedimientos establecidos para tal fin.

Respaldo de la información

Cada usuario deberá guardar y mantener una copia actualizada de su activo de la información en los servidores de archivos (o rutas compartidas por el Área de TI) dado que estos servidores cuentan con rutinas diarias de respaldo de información ante la presentación de cualquier tipo de incidente.

Monitoreo del uso de los sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través de los sistemas de información, u otros sistemas de comunicación de Loginter (incluidas las aplicaciones, correos electrónicos, entre otros) se consideran propiedad de Loginter por lo que este, en total cumplimiento, se reserva el derecho de monitorear y acceder al

contenido de todas y cada una de las comunicaciones electrónicas y telefónicas de los usuarios.

Instalación del software

La instalación de cualquier software no aprobado, es decir, aquel que no esté reconocido como parte de los sistemas necesarios para el negocio, estará estrictamente prohibida en los equipos que son de propiedad de Loginter o que están bajo su responsabilidad. Si por algún motivo se requiere la instalación temporal de un software que no esté previamente aprobado, deberá solicitarse al área de tecnología cumpliendo con el procedimiento establecido para tal fin.

Responsabilidad de las cuentas de usuario

El usuario debe abstenerse de permitir, de manera directa o indirectamente, que otras personas utilicen sus derechos de acceso. Esto significa que no está permitido ingresar a la red o sistemas con un nombre de usuario que no sea el propio.

DataCenter

El DataCenter posee controles de restricción de acceso físico, y solo las personas previamente autorizadas pueden tener acceso al mismo. El acceso de los visitantes o de terceros deberá realizarse únicamente con el acompañamiento de un empleado autorizado y cumpliendo con los protocolos definidos. El DataCenter se mantendrá limpio y organizado, y no se permitirá la entrada de alimentos, bebidas o materiales inflamables.

El DataCenter cuenta con equipos de protección física suficientes para garantizar la adecuada seguridad, tales como: sistema de detección y extinción de incendio automático, aire acondicionado con control de humedad/temperatura, alarmas de control de intrusión, incendio, racks de servidores y cableado protegido.

Acceso a Internet

- Cualquier información que se acceda, transmita, reciba o produzca en internet dentro de los equipos de Loginter puede ser objeto de auditoría.
- Los equipos, la tecnología y los servicios provistos para el acceso a internet son propiedad de Loginter, que puede analizar y si es necesario, bloquear cualquier archivo, sitio web, correo electrónico, dominio o aplicación almacenadas en la red internet o en las áreas privadas de la red, para garantizar el cumplimiento de la política de la seguridad de la información.
- Cualquier intento de cambiar los parámetros de seguridad por parte de cualquier empleado sin la debida acreditación y autorización para hacerlo se considerará inadecuado y los riesgos relacionados se informarán al empleado y su jefe inmediato o Gerente.

Ingeniería Social y Phishing

- Si el usuario no está seguro del origen de un enlace, correo electrónico u otra comunicación, el colaborador deberá buscar orientación y notificar inmediatamente al Área de Tecnología.

- Los colaboradores no deberán proporcionar su nombre o contraseña a través de ningún enlace de correo electrónico, llamada telefónica u otro método hasta que el solicitante este totalmente identificado y verificado.

Gestión de Dispositivos

Los dispositivos móviles incluyen todo tipo de computadoras portátiles, teléfonos celulares, smartphones, dispositivos USB, tarjetas de memoria y otros dispositivos móviles utilizados para almacenar, procesar y transferir datos.

Reglas básicas

• Los colaboradores deberán tomar precauciones cuando el dispositivo móvil se encuentra en automóviles u otro tipo de transporte, espacios públicos, habitaciones de hotel, lugares de reunión, centro de conferencias y otras áreas no protegidas fuera de las instalaciones de la organización.

• Los colaboradores, que retiren los dispositivos móviles de las instalaciones de Loginter, deberán tener en cuenta estas consideraciones:

- Los dispositivos móviles que contienen información clasificada como "confidencial", o de "uso interno" no deberán dejarse desatendidos y, si es posible, bloqueados físicamente.
- Cuando se utilicen dispositivos móviles en lugares públicos, el usuario deberá tener cuidado de que los datos no sean leídos por personas no autorizadas.
- El colaborador que utiliza dispositivos móviles fuera del sitio será responsable de realizar copias de seguridad periódicas de los datos en los repositorios compartidos de la compañía (servidor de archivos).
- La conexión a las redes de comunicación de la organización y el intercambio de datos deberá reflejar la confidencialidad de los datos y ser realizado a través del acceso VPN.
- La protección de datos confidenciales se deberá implementar de acuerdo con la clasificación de la información.

Uso de dispositivos removibles

- Los puertos USB de las estaciones de trabajo y laptops se encuentran deshabilitados por razones de seguridad. Para aquellos escenarios donde se requiere hacer el uso de estos, se deberá especificar los motivos y brindar una autorización del jefe o Gerente inmediato.
- Ante problemas, incidencias o señales del Malware, los dispositivos removibles USB deberán ser escaneados por el usuario con el antivirus local. Los dispositivos removibles deberán ser dedicados para el uso laboral, considerando que la información almacenada o transferencia es encriptada.

Uso de estaciones de trabajo

- Las estaciones de trabajo o notebooks deben ser utilizadas exclusivamente para llevar a cabo actividades relacionadas con el cumplimiento de los objetivos laborales de la organización.
- Cada usuario es responsable de preservar y cuidar los dispositivos y recursos proporcionados por la organización.

- En caso de daño, pérdida o falta de devolución de notebooks y/o sus accesorios, el Área de Recursos Humanos evaluará la situación y tomará las medidas adecuadas en función de las consecuencias que se presenten.

Cuidado de los equipos

- El usuario será responsable del almacenamiento y resguardo del dispositivo mientras está en su posesión, teniendo cuidado de preservar el dispositivo, evitando su exposición en entornos y situaciones que pueden afectar sus mecanismos de funcionamiento.

A modo de ejemplo, aquí hay algunas precauciones especiales para garantizar la conservación de su equipo:

- No limpiar la pantalla portátil con alcohol o productos equivalentes. La limpieza deberá hacerse preferiblemente con una franela.
- No dejar caer líquidos sobre el teclado. Los líquidos deberán permanecer alejados de su equipo.
- No conectar la computadora portátil a una toma de corriente sin verificar primero y asegurarse que tenga el voltaje adecuado.
- No forzar o conectar cables opcionales sin saber primero que son compatibles, evitando así daños a un puerto físico de su computadora portátil.
- No colocar objetos pesados encima del teclado.
- No golpear o dejar caer su dispositivo asignado (incluyendo hand helds, laptops, tablets y celulares, entre otros). Mantenga su dispositivo, así como sus cables o accesorios, en un lugar seguro y apropiado para evitar accidentes con las personas o con el dispositivo.

Gestión de Dispositivos

- El trabajo remoto significa que los dispositivos portátiles o de comunicación se utilizarán para permitir que los usuarios trabajen fuera de las instalaciones de Loginter. La concesión de acceso remoto deberá seguir el mismo proceso de gestión de acceso.
- La protección física de los dispositivos móviles.
- La prevención del acceso no autorizado por parte de personas que viven o trabajan en el lugar donde se realiza la actividad del trabajo remoto.
- La configuración de red adecuado utilizada para conectarse a Internet, bajo una red segura protegida por contraseña.

Ubicación de Escritorios y Equipos

- Los lugares de trabajo del personal de Loginter S.A. deben situarse en áreas no accesibles para personas externas, a excepción de las oficinas de atención al público. En estos casos, se debe colocar los monitores de manera que no sean visibles desde el exterior.

Escritorios Ordenados

- Cuando el personal se retire de su estación de trabajo, debe asegurar y cerrar con llave cualquier documento físico, medio magnético u óptico que contenga

información pública, interna o confidencial. Esto incluye la obligación de retirar inmediatamente la información confidencial impresa de las impresoras.

- En el caso del personal en áreas de atención al público, al ausentarse debe guardar también documentos y medios con información interna o confidencial.

- Al finalizar la jornada laboral, los colaboradores deben asegurar en un lugar seguro los documentos y medios con información interna o confidencial, y bloquear los equipos de cómputo. No basta con apagar el monitor; se debe bloquear el equipo utilizando, por ejemplo, las teclas Windows + L en sistemas operativos Windows.

Pantallas Limpias

- Las pantallas de las computadoras deben mantenerse libres de archivos o accesos directos. Estos deben organizarse en carpetas designadas para almacenamiento.
- Cuando el personal se ausente de su estación de trabajo, debe bloquear las sesiones de sus equipos de cómputo.
- Todos los equipos de cómputo y dispositivos portátiles deben tener activada la opción de cierre de sesión por inactividad, según las especificaciones del equipo de Sistemas.
- Al ausentarse, el personal debe bloquear todos los equipos y dispositivos bajo su responsabilidad.

Equipos de Reproducción de Información

- Los equipos de reproducción de información, como impresoras, fotocopiadoras y escáneres, deben ubicarse en áreas de acceso controlado. Cualquier documentación con información confidencial debe retirarse inmediatamente y guardarse en un lugar seguro.

Obligaciones

Los usuarios tendrán responsabilidades explicitas de seguridad de la información y deberán ser responsables de sus acciones. Parte del rol general de la administración será monitorear el cumplimiento de los requisitos de la presente política:

- Cada empleado tendrá la obligación de proteger la información de propiedad y de clasificarla correctamente, de acuerdo con lo establecido por Loginter; así como de proteger físicamente los activos. Por lo tanto, los ejemplos enumerados en esta práctica deberán usarse como una guía y aplicarse adecuadamente.
- En caso de dañar físicamente algún dispositivo, se le solicitara un informe del incidente suscitado (en caso necesario).
- Todos los empleados tendrán la responsabilidad continua de proteger la información, los datos, los elementos de infraestructura y los sistemas de soporte, y de garantizar la seguridad, la confiabilidad e integridad de las actividades de procesamiento de información y procesamiento de información.
- Las violaciones de cualquiera de las disposiciones anteriores deberán ser reportadas al responsable del Sistema de Gestión de Seguridad de la Información de la organización.

Cumplimiento
El cumplimiento de esta Política es mandatorio. En caso de infracción, Loginter se reserva el derecho de aplicar las medidas disciplinarias que correspondan, incluyendo la terminación de su relación laboral o contractual, en la medida en que lo permita la ley aplicable.

Ante cualquier inquietud o necesidad de más información sobre esta política, podés contactarte con:

Equipo de Gestión de Seguridad de la Información
SeguInfo@loginter.com.ar

Para realizar una denuncia de infracción sobre esta Política de manera anónima

canaldirecto@loginter.com.ar
0800-444-0522
www.loginter.com.ar/canal-directo