



POLITICA DE SEGURIDAD INFORMÁTICA

Versiones de este documento

Fecha	Quién	Versión	Descripción
18-diciembre-2019	Claudia Gómez	0,1	Draft inicial
5-octubre-2024	Claudio Bustos	0,2	Agrega sanciones por incumplimiento

Objetivos

ArticLYNX es una empresa de servicios informáticos, cuya labor se realiza en las dependencias de cada cliente, por tanto las políticas de seguridad informática describen la relación entre los colaboradores de la empresa, los activos informáticos y los clientes.

ArticLYNX se define a sí misma como una empresa en la nube, en el contexto de que toda la infraestructura necesaria para operar se encuentra en la nube (servicios de infraestructura, correo, gestión de identidad y acceso, servicios de almacenamiento, etc), es decir, sus políticas de seguridad informática son acorde a este enfoque de negocio.

Dada la naturaleza de nuestra labor como empresa, los colaboradores ArticLYNX se relacionan no sólo con activos informáticos de la empresa, sino que eventualmente con lo de los clientes, porque su labor principalmente se desarrolla en las dependencias de éstos últimos, por lo tanto, es necesario establecer las políticas de seguridad de uso de activos informáticos tanto los de ArticLYNX como los de sus clientes.

El objetivo de este documento es establecer y difundir el cumplimiento de buenas prácticas en el uso de los activos informáticos, tanto para ArticLYNX, como para nuestros clientes.

Definiciones

Clasificación de la Información

Todos los datos de propiedad de ArticLYNX, de sus clientes y de sus proyectos se deben clasificar dentro de las siguientes categorías: CONFIDENCIAL, PRIVADO y PÚBLICO.

Para identificar la naturaleza de la información, los colaboradores ArticLYNX deben ceñirse a los siguientes criterios:

- **CONFIDENCIAL:** La información contenida es acerca de ArticLYNX, de sus clientes o de los proyectos y NO debe ser leída por personas distintas a los destinatarios o para los que se generó dicha información.
- **PRIVADO:** La información contenida es de uso personal, distinto de los intereses de ArticLYNX, de sus clientes o de sus proyectos.
- **PÚBLICO:** La información contenida es acerca de ArticLYNX, de sus clientes o de los proyectos y NO reviste ningún riesgo de seguridad el que sea leída por un tercero. Esta es el tipo más común de información generada y recibida en la empresa, usualmente versa sobre actividades de los proyectos ejecutados en los clientes de ArticLYNX.

Políticas de Seguridad Informática

Políticas Generales

- Todos los colaboradores ArticLYNX deben comprender las políticas de seguridad de informática descritas en este documento.
- Este documento tendrá una versión actualiza en:
 - https://www.alx.cl/politicas_seguridad_informatica_ArticLYNX.pdf
- Todos los colaboradores ArticLYNX, para su ejercicio, deben tener firmado el acta de aceptación de las políticas de seguridad informática descritas en este documento.

Almacenamiento de Información

- Todos los datos de propiedad de ArticLYNX, de sus clientes y de sus proyectos deben ser almacenados en servicios de Nube provisto por la empresa y por tanto NO deben ser almacenados en lugares distintos a estos:
 - One Drive
 - SharePoint
 - iCloud Drive
 - DropBox
- Los datos de propiedad de ArticLYNX, de sus clientes y de sus proyectos NO deben ser impresos en papel y en caso de que fuera estrictamente necesario, debe ser notificado a la jefatura, indicando qué, cuándo, por qué y quienes son los involucrados.
- En general, NINGÚN dato de ArticLYNX, de sus clientes y de sus proyectos debe ser almacenado en forma de papel ni en otro mecanismo que no sean los descritos en esta política de almacenamiento.

Correos electrónicos

- Todos los colaboradores ArticLYNX deben usar un certificado válido MIME correctamente instalado y configurado en sus herramientas de correo electrónico que les permita tanto firmar como cifrar electrónicamente los mensajes de correo.
- Todo correo cuya información es clasificada como CONFIDENCIAL, debe ser firmada y cifrada para los colaboradores ArticLYNX y en general para todo destinatario que cumpla con el certificado MIME.
- Todo correo cuya información es clasificada como CONFIDENCIAL, debe ser etiquetado al inicio del asunto como “CONFIDENCIAL: ”.
- Todo correo cuya información es clasificada como PRIVADO, debe ser etiquetado al inicio del asunto como “PRIVADO: ”
- Todo el correo entrante y saliente debe ser respaldado por la empresa, con una retención mínima de 3 meses.

Equipos de hardware

- Todos los equipos de hardware, ya sean de ArticLYNX o propios de los colaboradores, que sean usados para actividades de la empresa, DEBEN usar un mecanismo de cifrado de TODOS sus discos.
- Todos los equipos móviles como teléfonos inteligentes o tablets, ya sean de ArticLYNX o propios de los colaboradores, que sean usados para actividades de la empresa, DEBEN estar enrolados en el servicio de nube Intune de ArticLYNX.
- Todos los equipos de cómputo, que sean usados para actividades de la empresa, deben poseer un antivirus activo y actualizado.
- El sistema operativo de cada equipo de cómputo, ya sea de escritorio, laptop, equipo móvil o servidor DEBEN estar actualizados en sus parches de seguridad provistos por el fabricante del sistema operativo.
- Todo sistema operativo usado en la empresa, ya sea de escritorio, laptop, equipo móvil o servidor debe estar provisto de soporte por el fabricante del sistema operativo.
- Dada la naturaleza del ámbito profesional de los colaboradores de ArticLYNX, es que ellos mismos DEBEN hacer mantención a sus equipos de hardware para hacer cumplir estas políticas.
- Todos los equipos de computo, que sean usados para actividades de la empresa, DEBEN estar físicamente bajo el control del colaborador que lo posea. Esto es, que el colaborador sepa y esté consciente en todo momento de la ubicación física del equipo y que a su vez, cuando sea almacenado, se haga en un lugar donde se minimice el riesgo de acceso al equipo por terceros no autorizados. Esto involucra, por ejemplo, que en los viajes el equipo debe ser parte del equipaje de mano y no de bodega.
- Toda pérdida de control sobre el equipo de hardware por parte del colaborador que lo posea DEBE ser notificada a su jefatura inmediatamente. Esto involucra pérdidas, robos o cualquier siniestro. Esta actividad es de vital importancia porque permite a la empresa hacer gestión sobre los datos que posea ese equipo a fin de minimizar los riesgos de accesos por terceros a la información

que pudiera estar almacenada en el equipo siniestrado.

Respaldos y Recuperación ante Desastres

- Todo servicio de nube que almacene datos e información de la empresa y de sus clientes debe ser respaldado diariamente y cifrado en otro servicio de nube.
- Cada servicio respaldado DEBE poseer un plan de recuperación en caso de desastre.

Propiedad Intelectual

- Todos los datos, información, documentos generados a raíz de las actividades propias de los proyectos de ArticLYNX con sus clientes o de actividades propias, pertenecen a ArticLYNX, es decir, la empresa posee todos los derechos de propiedad intelectual sobre ellos.
- Toda obra, diseño, codificación, código fuente desarrollado, mecanismo, metodología, técnica, artefacto y herramientas creadas en el ejercicio de las actividades propias de la empresa pertenecen a ArticLYNX, por lo tanto, la empresa posee todos los derechos de propiedad intelectual sobre ellos.

Control de la Información

- Aunque toda la infraestructura operacional de ArticLYNX se encuentra en la nube, como gestión de identidades de usuarios, credenciales y derechos de acceso, los usuarios NO deben intentar sobrepasar los controles de los sistemas para escalar u obtener accesos a activos para los que NO posean accesos.
- Los usuarios DEBEN informar a su superior ante un evento que comprometa alguna de las políticas descritas en este documento para su oportuna solución y resguardo de los activos.
- Los usuarios DEBEN informar a su superior ante un evento de virus o malware informático descubierto en algún equipo de cómputo en los que se procese información de la empresa, de sus clientes o de proyectos.
- Los colaboradores NO deben suministrar cualquier información de la empresa, de sus clientes o de sus proyectos a ningún agente externo sin las autorizaciones respectivas.
- Toda divulgación de información CONFIDENCIAL a terceras personas debe estar acompañada previamente por un contrato que describa explícitamente qué información es restringida y cómo puede o no ser usada. Esto es, ANTES de poder compartir información confidencial de ArticLYNX, de sus clientes o de sus proyectos con un tercero, ya sea esta persona natural o jurídica, se debe firmar un acuerdo de NO divulgación de datos o información para proteger de fugas no controladas desde la empresa.
- Toda información CONFIDENCIAL generada y/o almacenada producto de proyectos de ArticLYNX con sus clientes y que no revistan de utilidad funcional para soporte o garantías DEBE ser eliminada de TODO almacenamiento de ArticLYNX (nube, equipos de colaboradores, almacenamientos externos, correos, etc) una vez que el proyecto cierre. Es permisible que esos datos permanezcan en los respaldos de la información del proyecto y se asume que serán eliminados definitivamente una vez que los tiempos de retención de dichos respaldos se cumplan.

Control del Software de la Empresa

- ArticLYNX debe contar en todo momento con un inventario actualizado del software de su propiedad ya sea desarrollado, licenciado, arrendado o comprado para que los colaboradores estén al tanto de los softwares que pueden usar. Dicho inventario estará siempre disponible en https://www.alx.cl/inventario_sw.php
- Todo Software usado en la empresa DEBE poder administrar roles y niveles de acceso de tal manera de poder entregar los niveles adecuados de privilegios de acuerdo a las labores encomendadas a cada colaborador.
- Todos los servicios de Nube deben proveer de un mecanismo centralizado y único de administración de Identidades y accesos para conformar un directorio (Active Directory) de todo ArticLYNX en la Nube, accesible de cualquier lugar, en cualquier horario y con garantías de alta disponibilidad que garanticen el funcionamiento en todo momento de ese servicio.

Sanciones por incumplimiento

Los colaboradores de ArticLYNX deben guardar cumplimiento y observación a lo dispuesto en este documento. Las sanciones que no sean causales de término de contrato de trabajo, serán sancionadas en distintos grados, según la evaluación del caso, de los cuales se llevará registro en el sistema de información interno.

Los grados de amonestación serán:

- **Advertencia Verbal o Escrita:** Para infracciones menores o primeras ofensas, se puede emitir una advertencia al colaborador, recordándole la importancia de cumplir con las políticas de seguridad. Esta sanción debe ir acompañada por una amonestación escrita sin copia a la hoja de vida.
- **Revocación de Accesos:** Se pueden restringir o revocar los accesos del colaborador a ciertos sistemas, aplicaciones o datos sensibles para prevenir futuros riesgos de seguridad. Esta sanción debe ir acompañada por una amonestación escrita con copia a la hoja de vida.
- **Terminación del Contrato de Trabajo:** En casos graves, especialmente si el incumplimiento ha causado daños significativos o violaciones legales, el colaborador puede ser desvinculado de la empresa.
- **Acciones Legales:** Si el incumplimiento involucra actividades ilegales, como robo de datos, espionaje corporativo o divulgación de información confidencial, la empresa puede emprender acciones legales contra el colaborador.
- **Notificación a Organismos Regulatorios:** En ciertos casos, especialmente si hay implicaciones legales o regulatorias, la empresa puede estar obligada a informar a las autoridades competentes.