Políticas de Seguridad Informática Álaga

Responsabilidades de los clientes o usuarios

Nuestro sitio cuenta con certificado SSL (Secure Sockets Layer, en sus siglas en inglés) el cual nos permite encriptar los datos mientras viajan desde el computador de nuestros clientes o usuarios hasta nuestro servidor, de esta forma nadie podrá interceptar la comunicación para apoderarse de sus datos personales.

No obstante lo anterior, es una responsabilidad de nuestros clientes o usuarios implementar los controles de seguridad necesarios, en sus equipos y redes privadas para su navegación hacia el portal de Álaga o para el envío de correos electrónicos.

El usuario o cliente deberá atender las siguientes prácticas:

- El cliente o usuario se compromete a tener instalada y actualizados sistemas de Antivirus y anti espionaje que le permitan mitigar el impacto de posibles ataques.
- Es deseable que el cliente o usuario mantenga esquemas Firewall que generen mayores niveles de seguridad en sus transacciones.
- El cliente o usuario se compromete a mantener actualizados los dispositivos de conexión y a instalar las actualizaciones de las aplicaciones o sistemas que disponible Álaga con el fin de garantizar la renovación de todos los componentes de seguridad de las mismas.
- En todo caso, el cliente o usuario deberá garantizar la conexión a través de redes seguras que garanticen la mitigación de probabilidad de ataques externos

Gestión de contraseñas:

- La contraseña con la cual el cliente o usuario ingresa y utiliza los servicios del Micrositio es de uso personal e intransferible. El cliente o usuario se obliga a mantenerla bajo absoluta reserva, a fin de que nadie más tenga acceso a los servicios ofrecidos.
- El cliente o usuario autoriza que, con el ingreso de su contraseña, las operaciones que este realice a través del Micrositio se efectúen automáticamente una vez Álaga S.A.S. compruebe su contraseña y los datos del mismo.
- El cliente o usuario será responsable de los daños y perjuicios que pueda causar a Álaga S.A.S. o a cualquier tercero por los usos indebidos del Micrositio.
- Las contraseñas deben tener como mínimo 8 caracteres de longitud.
- Las contraseñas deben tener dígitos numéricos, mayúsculas, minúsculas y caracteres especiales.
- Los clientes o usuarios deben cambiar la contraseña cada vez que el sistema se lo solicite o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad • No se pueden establecer contraseñas que correspondan a secuencias básicas del teclado (“qwerty”, “1234”, “98765”).
- No se pueden reutilizar contraseñas pasadas cuando el sistema solicite un cambio de contraseña.
- Las contraseñas no deben contener el nombre del usuario del cliente o usuario.
- Las contraseñas no pueden ser compartidas, genéricas o para grupos.
- Los clientes o usuarios no deben revelar sus contraseñas con terceros.
- Los clientes o usuarios no escribirán sus contraseñas en correos electrónicos, formularios web o redes sociales. Álaga no pedirá por ningún medio compartir este tipo de información de parte de sus Clientes o usuarios.

Responsabilidades de los colaboradores

- Utilizar solamente los repositorios de información definidos por el dueño del proceso y dispuestos por la organización para el almacenamiento y custodia de información.

- Los repositorios definidos por la organización son única y exclusivamente para almacenar información de la organización.

- Proteger y tratar la información que administran en el desempeño de sus funciones de acuerdo con su clasificación.

- Realizar respaldos periódicos de la información almacenada en el equipo asignado de la empresa, utilizando las herramientas y repositorios corporativos dispuestos por la organización.

- Para la información clasificada como personal, sensible, confidencial e interna que requiera ser suministrada a un tercero debe contar con la aprobación del dueño del proceso y adicionalmente previo al envío, consultar con el encargado de control interno y tecnología del negocio quienes le indicarán las medidas de seguridad requeridas para el suministro de esta información.

- Para la información clasificada como personal, sensible y confidencial que requiera ser suministrada a un tercero, debe contar con las aprobaciones indicadas en la tabla de gestión documental y adicionalmente previo al envío, consultar con el encargado de control interno y tecnología del negocio quienes le indicarán las medidas de seguridad requeridas para el suministro de esta información.

- Asegurar que los contratos con terceros cuenten con las cláusulas establecidas para el tratamiento adecuado de la información.

- Aplicar las condiciones de seguridad de la información en el intercambio de ésta con terceros (proveedores, socios de negocio, contratistas) con base en la clasificación y etiquetado de la información.

Segregación de funciones

Toda tarea en la cual los colaboradores tengan acceso a la infraestructura tecnológica debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir la concentración de funciones y evitar el uso no autorizado o modificación sobre los activos de información de la Compañía.

Aspectos de seguridad para proteger la información digital

Todos los usuarios de los sistemas de información deben tener una identificación personal e intransferible (cuenta y contraseña) para hacer uso de la información y de los recursos tecnológicos.

Toda contratación con terceros que implique entrega o intercambio de información de la compañía debe estar respaldada con una cláusula de confidencialidad establecida en el contrato, o un acuerdo de confidencialidad cuando aplique.