

DECLARACIÓN DE INTENCIONES

“La información relacionada con nuestros clientes, proveedores y los servicios que les prestamos es, por principio y esencia del objetivo de negocio de intermediación entre constructoras y suministradores de trabajos relacionados con el sector de la construcción, el activo principal de Construred.

El afianzamiento y respaldo de la confianza que en nosotros ya han depositado nuestros clientes se basa en la adhesión a los principios fundamentales de la seguridad de la información (Integridad, Disponibilidad y Confidencialidad) y al cumplimiento estricto de las políticas, normas y procedimientos que garanticen una seguridad sistemática, adecuada, eficaz y continua.”



José Luis Ramiro Oter

Director CONSTRURED, Construcciones y transacciones electrónicas en la red, S.L.

PRINCIPIOS DE LA ORGANIZACIÓN RESPECTO A LA SEGURIDAD

Concienciación: Los empleados y contratados deben ser conscientes de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad.

Responsabilidad: Todos los empleados son responsables de la seguridad de los sistemas de información y redes.

Respuesta: Los empleados actuarán de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten la seguridad.

Ética: Los empleados respetarán los intereses legítimos de los otros, y seguirán el código ético de Construred.

Democracia: La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática

Evaluación del riesgo: Los empleados deben llevar a cabo evaluaciones de riesgo en sus áreas funcionales.

Diseño e implementación de la seguridad: La seguridad de la información se gestionará como un elemento esencial de los sistemas de información y redes.

Administración: Los empleados deben adoptar una visión integral de la administración de la seguridad.

Evaluación: Se revisará y reevaluará la seguridad de los sistemas de información y redes, implantándose las modificaciones pertinentes a las políticas, prácticas, medidas y procedimientos de seguridad.

DIRECTRICES DE SEGURIDAD

- Se debe nombrar oficialmente, siendo comunicado de manera fehaciente a todos los empleados de la Organización, una persona como RESPONSABLE DE SEGURIDAD para gestionar y administrar los riesgos, requisitos, incidencias y mejoras en seguridad mediante un Sistema de Gestión de la Información que Construred ha diseñado apoyándose en la metodología de Adhoc Security, y del que este documento forma parte.
- Se deben diseñar unos procedimientos estándares de intercambio, acceso y almacenamiento seguro de la información de nuestros clientes y proveedores, que aseguren el cumplimiento de los objetivos de seguridad en cuanto a su confidencialidad, disponibilidad e integridad, dentro de las posibilidades de la técnica.
- La entrada, salida y procedimientos de trabajo de los empleados en el entorno de la empresa debe seguir unas pautas seguras definidos en normas de seguridad que se les comunicarán.
- Los empleados aceptarán formalmente el Código ético de la empresa y cualquier manual de uso de recursos que Construred les haga llegar.
- Se deben definir metodologías de desarrollo seguro de aplicaciones informáticas de gestión o de plataformas teniendo en cuenta los objetivos de seguridad definidos por la organización, así como las contramedidas que análisis de riesgos pudieran recomendar.
- Los sistemas y redes informáticas seguirán unas normas de protección adecuadas a los objetivos de seguridad determinados y nivel de riesgo decidido a gestionar.
- Se debe diseñar y mantener un plan de continuidad de los procesos internos y de la plataforma tecnológica de gestión del negocio para soportar cualquier desastre, sin perjuicios graves y duraderos para nuestros empleados, nuestros clientes, nuestros activos de negocio y, en definitiva, nuestra empresa.

OBJETIVOS DE SEGURIDAD

Así mismo, en base a la tipología de los activos de información considerados más críticos para el proceso de negocio, se deben tener en cuenta estos criterios de cara a la gestión de contramedidas:

- **DISPONIBILIDAD DE LA INFORMACIÓN:** toda la información relativa a clientes (tanto de constructoras como de proveedores asociados) tratada a través de la página Web corporativa, deberá estar en todo momento disponible, lo que supone la implantación de todas aquellas medidas técnicas y de procedimiento que se consideren necesarias garantizar este objetivo.

Una indisponibilidad de la misma por un período superior a 24 horas supondría un quebranto de los objetivos de seguridad de Construred, con las consiguientes consecuencias contractuales y de imagen para la empresa.

Respecto a la información tratada en la plataforma Proforma, el período máximo de indisponibilidad se establece en 12 horas.

- **INTEGRIDAD DE LA INFORMACIÓN:** se pondrán todos los medios posibles para evitar pérdidas parciales y/o totales de los activos de información, tanto los disponibles en la página Web, como los soportados por las aplicación Proforma.