POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de la política de seguridad de la información es proteger los recursos incluidos en el SGSI (Sistema de Gestión de la Seguridad de la Información) de las amenazas (internas, externas, deliberadas, accidentales) que puedan comprometerlos, garantizando principalmente la Confidencialidad, Integridad y Disponibilidad de la información.
En particular, para todos los sistemas bajo el SGSI, la organización debe asegurar que

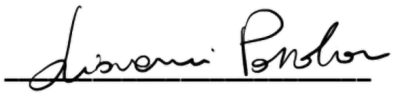
- La información es accesible únicamente a las personas autorizadas, tanto internas como externas a la empresa, garantizando niveles de servicio y complejidad compatibles con los requisitos funcionales de los sistemas en cuestión;
- Cualquiera que sea el formato de la información tratada, se garantiza su disponibilidad, integridad y confidencialidad en cumplimiento de los requisitos legislativos aplicables;
- Se lleva a cabo una supervisión constante de los activos y la tecnología cambiantes para identificar rápidamente las nuevas vulnerabilidades;
- Se lleva a cabo una supervisión constante de los activos y la tecnología cambiantes para identificar rápidamente las nuevas vulnerabilidades.
- Se presta especial atención a los cambios en los requisitos y prioridades reglamentarias y contractuales en relación con los nuevos desarrollos de aplicaciones;
- La continuidad de la actividad se garantiza mediante intervenciones organizativas y tecnológicas específicas, y que estas intervenciones se definen, se actualizan constantemente y se verifican periódicamente;
- Que todo el personal reciba formación en materia de seguridad, que se le informe de la obligatoriedad de las políticas de la empresa a este respecto y que también se le hagan saber las consecuencias de infringir las políticas de la empresa;
- Las evaluaciones periódicas de la eficacia del SGSI y de la formación del personal se llevan a cabo mediante simulaciones en el ámbito de aplicación (pruebas de penetración/intrusión de la seguridad lógica/física, pruebas de conocimiento de las políticas y simulaciones de violaciones de las mismas);
- Se introducen métricas para evaluar el rendimiento del sistema;
- Las tareas relacionadas con las actividades críticas están separadas (por ejemplo, el desarrollo y las pruebas con la producción);
- Los riesgos se reducen al máximo en su origen;
- Cualquier violación de la seguridad, real o presunta, se comunica e investiga;
- Los incidentes de seguridad se identifican y gestionan rápidamente, y las autoridades competentes se activan para aquellos que repercuten en la violación de los requisitos legales;
- Se impide el uso de software no autorizado;
  Se realizan revisiones periódicas del SGSI con respecto a:
  - verificación de la pertinencia y la eficacia de los controles aplicados para las amenazas y vulnerabilidades identificadas en el plan de tratamiento de riesgos;
  - impacto de los controles implementados en la eficacia de la gestión;
  - los cambios provocados por la tecnología (vulnerabilidades nuevas o modificadas, reducción del riesgo debido a los nuevos conocimientos adquiridos como resultado del progreso tecnológico);
  - los cambios realizados en la configuración de los sistemas del SGSI;
  - reevaluación periódica del riesgo y, en particular, de las acciones preventivas.

También se define la metodología de evaluación de riesgos basada en las directrices de la norma ISO/IEC 27005. Para supervisar el rendimiento del sistema, se han identificado objetivos de seguridad, que se miden mediante KPI específicos indicados en el documento: ISMS_110.IT.0-Security Objectives KPI.

La responsabilidad del establecimiento y la gestión del SGSI se asigna al responsable de la seguridad de la información.

Villorba, 01/06/2022

Security Manager
Giovanni Pozzobon



CEO
Giorgio De Nardi