Anexo E – Gestión de roles y responsabilidades

1. Responsable de Seguridad

El Responsable de Seguridad es la figura personal más importante en el desarrollo de la seguridad de la información. Este rol, será asumido por el responsable del área de TI, que delegará algunas de sus actuales responsabilidades en el personal que tiene debajo de él jerárquicamente para poder asumir el nuevo rol. Además, recibirá la formación pertinente para este rol.

Sus responsabilidades en materia de seguridad de la información serán las siguientes:

- Elaborar, promover y mantener la política de seguridad de la información.
- Elaborar el plan de riesgos y las posibles soluciones para mitigar las amenazas.
- Proponer nuevos objetivos en materia de seguridad de la información.
- Desarrollar y mantener el marco normativo de seguridad y controlar su cumplimiento.
- Validar la implantación de los requisitos de seguridad necesarios.
- Liderar la implantación del SGSI.
- Establecer los controles y medidas técnicas y organizativas para asegurar los sistemas de información.
- Gestionar la seguridad de la información de la organización de manera global.
- Gestionar y analizar las incidencias de seguridad que tienen lugar en la organización.
- Revisar periódicamente el estado de la seguridad de la información.
- Realizar el seguimiento de los incidentes de seguridad.
- Controlar y revisar los indicadores definidos.
- Controlar que las auditorías de seguridad se realicen con la frecuencia necesaria.
- Revisar los informes de auditoría.

- Definir y comprobar la aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidencias.
- Reportar al Comité de Seguridad las cuestiones relevantes en materia de seguridad de la información.

2. Comité de seguridad

El comité de seguridad de Ícaro S.A. son las siguientes:

- Responsable de seguridad
- Director General
- Director de Operaciones
- Director Técnico

Las funciones y responsabilidades del Comité de Seguridad son:

- Implantar las directrices de la Dirección.
- Asignar los distintos roles y funciones en materia de seguridad.
- Presentar las políticas, normas y responsabilidades en materia de seguridad de la información a la Dirección para que sean aprobadas.
- Validar el mapa de riesgos y las acciones de mitigación propuestas.
- Validar el Plan de Seguridad y presentarlo a la Dirección para que sea aprobado.
- Supervisar el desarrollo y mantenimiento del Plan de Continuidad de negocio.
- Velar por el cumplimiento de la legislación y regulación vigente.
- Promover la concienciación y formación de los empleados en materia de seguridad de la información.
- Aprobar y revisar periódicamente el cuadro de mando de la seguridad de la información y de la evolución del SGSI.

3. Funciones y responsabilidades del resto de personal

3.1 Personal con perfil de usuario

El personal con perfil de usuario es todo aquel que usa los sistemas de la información de la empresa para realizar su actividad profesional, pero no realiza ninguna gestión o administración ni tiene los privilegios para hacerlo. Este personal tiene las siguientes normas y responsabilidades:

- Respetar y seguir las normas y procedimientos definidos en la política de seguridad de la empresa.
- Mantener la confidencialidad de la información.
- Hacer un buen uso de los activos de la organización.
- Respetar la legislación y regulación vigentes.
- Notificar al responsable de seguridad de las anomalías o incidentes de seguridad, así como las situaciones sospechosas.

3.2 Personal con acceso privilegiado

En la empresa hay cinco integrantes del departamento de TI con acceso privilegiado a los sistemas de información. Dos personas dedicadas a la administración de servidores y virtualización del sistema sirio, otras dos personas dedicadas a puesto de trabajo y los sistemas corporativos y una última persona como responsable del departamento de TI y Responsable de Seguridad. Estos perfiles tienen acceso de administrador a los sistemas de información, tanto equipos de usuario como, sistemas de centro de datos y acceso físico a las áreas restringidas relacionadas con los sistemas de información (CPD).

A continuación, se describe en detalle las funciones y obligaciones de cada perfil:

Administrador de puesto de trabajo y sistemas corporativos

Funciones:

- Mantenimiento Software y Hardware de los equipos de usuario (PC's, Teléfonos, Smartphone, Impresoras, Red, etc.).

- Administración del directorio activo de la empresa. Realiza el alta, baja y modificaciones de usuarios, así como de la administración de los roles.
- Administración sistema de correo electrónico corporativo. Realiza las tareas de administración de los buzones, altas, bajas y modificaciones de los usuarios, etc.
- Administración sistema de web corporativo
- Administración de los sistemas de ficheros de usuarios interno y externo.
- Administración de la BBDD corporativa.
- Administración del sistema CAS
- Administración del ERP.
- Administración y gestión de todos los servidores que soportan los sistemas corporativos.
- Colaborar con los administradores de servidores y virtualización del sistema Sirio.

Para este personal se describen las siguientes obligaciones, además de las anteriores que aplican al resto de usuarios:

- Promover la incorporación de mecanismos de integridad, autentificación, control de acceso y auditoría en el diseño, implantación y operación de los sistemas de información.
- Asegurar la confidencialidad y disponibilidad de la información almacenada en los sistemas de información, así como su salvaguarda mediante copias de seguridad periódicas.
- Conceder a los usuarios los privilegios mínimos que les permitan acceder a los datos y recursos necesarios para el desarrollo de sus tareas.
- No acceder a datos aprovechando su privilegio sin autorización del jefe de Departamento de TI o el responsable de seguridad.
- Custodiar con especial cuidado los identificadores y contraseñas que dan acceso a los sistemas con privilegios de administrador.
- Notificar las incidencias oportunas ante cualquier violación de las normas de seguridad vulnerabilidades detectadas en los sistemas.
- No revelar a terceros ninguna posible debilidad en materia de seguridad de los sistemas sin previa autorización del jefe del Departamento de TI o del responsable de seguridad.

Administradores de servidores y virtualización del sistema Sirio.

Funciones:

- Administración de la cabina de almacenamiento que almacena los datos del sistema sirio, así como las electrónicas de red SAN que da acceso a la misma.
- Administración del entorno de virtualización.
- Administración y gestión de los servidores físicos que soportan el sistema Sirio
- Administración de la electrónica de red de todo el CPD así como de los elementos de seguridad.
- Dar soporte al equipo de administradores del sistema software de Sirio.
- Colaborar con los administradores de puesto de trabajo y sistemas corporativos en momentos puntuales.

Para este personal se aplican las mismas obligaciones que a los administradores de puesto de trabajo y sistemas corporativos, así como las que aplican al resto de usuarios.