|  |  |  |
| --- | --- | --- |
| **Asignatura** | **Datos del alumno** | **Fecha** |
| **Sistemas de Gestión de la Seguridad de la Información** | Apellidos: Paz López | 16 de Junio del 2021 |
| Nombre: Angel Ramón |

**INTRODUCCION**

Hoy en día con la evolución de la tecnología y el crecimiento de las redes han traído cosas positivas en muchos aspectos, desde la comunicación, compartir recursos, haciendo eficientes ciertas actividades entre otros, pero también ha traído cosas negativas como ser la brecha de seguridad de la información abriendo paso a ataques en la red de hacker o personas con conocimientos informáticos con el objetivo sea para robar, acceder a redes privadas de una organización para tener acceso al principal activo de este como lo es la información. Es por eso que las organizaciones deben tener como objetivo principal la implementación de un Sistema de Gestión de Seguridad de la información, estableciendo controles y mecanismos de seguridad cuyo objetivo es mantener seguros los procesos y activos de la organización brindando confidencialidad, privacidad, integridad y disponibilidad de la información.

Y como soluciones tenemos normas, estándares, modelos y guías que nos ayudaran a implementar según sea el caso, un sistema de gestión para protección de la información como lo es ITIL / ISO 27001 / OISM3 en la cual este trabajo explicaremos en un cuadro comparativo las funciones de cada uno, su audiencia, su finalidad, y sus relaciones.

Análisis comparativo ITIL/ISO 27001/OISM3

|  |  |  |  |
| --- | --- | --- | --- |
| CRITERIOS | ITIL | ISO 27001 | OISM3 |
| Función | Recoger todas las prácticas que funcionan para la gestión de servicios de la tecnología de Información | Describe todos los requisitos de un Sistema de Gestión de la Seguridad de la Información proporcionando un marco para la elaboración de las normas de seguridad de una organización, estableciendo métodos de gestión eficaz de la seguridad | Permite el diseño de los sistemas de gestión de la seguridad alineados con los objetivos y la misión de la organización, la cual permite a estas priorizar y optimizar las inversiones en seguridad de la información, como también permitir la mejora continua de los sistemas de seguridad. |

|  |  |  |  |
| --- | --- | --- | --- |
| CRITERIOS | ITIL | ISO 27001 | OISM3 |
| Audiencia | A organizaciones o personas que estén relacionados con los entornos y TI. Orientada a procesos | Cualquier tipo de organización. Orientada a Controles | A organizaciones maduras. Orientada a Procesos |
| ¿Para qué es Implementado’ | Para mejorar la calidad de la gestión de servicios de tecnologías de la información | Para describir los requisitos de un Sistema de Gestión de la Seguridad de la Información | Para garantizar la implementación de los procesos y controles de seguridad en cualquier organización |
| ¿Qué es? | Es una guía de buenas Practicas | Es un Estándar Internacional – Requerimientos del SGSI | Es un Modelo de Madurez |
| Relación | El proceso de Seguridad de ITIL se basa en la norma ISO 27001 | Para mejorar los sistemas basadas en esta norma se puede usar O-ISM3 | O-ISM3 puede usarse para mejorar sistemas basados en ITIL, ISO27001 |

**CONCLUSION**

Las organizaciones tienen las herramientas necesarias para poder proteger sus procesos, sistemas de información y sus activos más valiosos, lo único que tienen que hacer es tener compromiso y entender que la seguridad de la información es muy valiosa implementarla si no estarían sometiendo a varios riesgos no deseados. Y como vimos en el Cuadro comparativo tenemos las Practicas de ITIL Fundado por OGC que es una guía de buenas practicas para aquellas organizaciones que estén relacionados en los entornos de la Tecnología de la Información la cual la organización podrá mejorar la calidad de la gestión de los servicios de la tecnología de la información, el proceso de Seguridad de ITIL se basa en la norma ISO 27001. El estándar ISO 27001 nos describe todos los requisitos para poder implementar un sistema de gestión de la seguridad de la información, estableciéndonos un marco para elaborar y planificar las normas de seguridad y políticas para tener una gestión eficaz de la seguridad. El O-ISM3 fundado por OPEN GROUP es un modelo de madurez para organizaciones maduras orientada a procesos ya establecidos, la cual garantiza la implementación de los procesos y controles de seguridad en cualquier organización, este modelo de madurez puede utilizarse para mejorar los sistemas basados en ITIL e ISO27001. Estas normas y estándares una vez implementados de forma eficaz cumplirán los objetivos de la organización manteniendo sus procesos, servicios y activos valiosos protegidos contra cualquier riesgo o evento no deseado.

**REFERENCIAS**

¿Qué es ITIL y para qué sirve? | GlobalSUITE Solutions. (2020, noviembre 12). *GlobalSUITESolutions*. https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/

*O-ISM3 v2.0 Executive Summary.pptx*. (s. f.). Google Docs. Recuperado 16 de junio de 2021, de https://docs.google.com/presentation/d/e/2PACX-1vTCxEkVxwatASHHg6R4IXuZ0FONWLUm5F1cIz\_TtX7u8zqyV4PtCrcbNe3l4I19hHYaBrZtEGG\_ULqv/embed?start=true&loop=false&delayms=3000&usp=embed\_facebook

Sistema de gestión de la seguridad de la información. (2021). En *Wikipedia, la enciclopedia libre*. https://es.wikipedia.org/w/index.php?title=Sistema\_de\_gesti%C3%B3n\_de\_la\_seguridad\_de\_la\_informaci%C3%B3n&oldid=133347065

*UNIR - TEMA 2—EL PROFESIONAL DE LA SEGURIDAD DE LA INFORMACIÓN*. (s. f.). Recuperado 16 de junio de 2021, de https://micampus.unir.net/courses/17652/external\_tools/95196