NORMATIVA DE CIBERSEGURIDAD

Unidad 2. Actividad 2

29 DE NOVIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado.

Basándote en nuestro Centro Educativo, haz una relación de todos los documentos que establecerías para la gestión del compliance con un enfoque integrador, descripción funcional, estructura o formato, clasificación (pertenencia a áreas) , relación con otros, control de acceso, etc.

Compliance. Seguridad informática.

Documentos Descriptivos:

Manual de Seguridad Informática:

- Descripción Funcional:

Define los principios y estándares de seguridad informática del centro educativo.

- Estructura o Formato:

Introducción, Objetivos, Políticas Generales, Normas de Acceso, Procedimientos de Seguridad, y Referencias.

- Clasificación (Pertenencia a Áreas):

Puede clasificarse como un documento de políticas institucionales y un componente clave del manual de la organización.

- Relación con Otros:

Se relaciona con el código de ética, protocolos de respuesta a incidentes y políticas específicas de sistemas.

Protocolo de Respuesta a Incidentes:

- Descripción Funcional:

Establece un marco para responder eficazmente a incidentes de seguridad informática.

- Estructura o Formato:

Definición de Incidentes, Proceso de Respuesta, Roles y Responsabilidades, y Evaluación Post-Incidente.

- Clasificación:

Pertenecerá al área de seguridad de la información y puede vincularse con el plan de continuidad del negocio.

- Relación con Otros:

Conectado con el manual de seguridad informática y las políticas de gestión de incidentes.

Código de Seguridad de la Información:

- Descripción Funcional:

Establece normas éticas y comportamientos relacionados con la seguridad de la información.

- Estructura o Formato:

Declaración de Principios, Normas de Conducta, Responsabilidades y Sanciones.

- Clasificación:

Pertenece al área de ética y comportamiento organizacional.

- Relación con Otros:

Está vinculado con el manual de seguridad informática y se refiere a políticas específicas.

"Welcome Packages" de Seguridad Informática:

- Descripción Funcional:

Facilita la integración de nuevos miembros al entorno seguro desde el principio.

- Estructura o Formato:

Mensaje de Bienvenida, Resumen de Políticas, Recursos de Formación, y Contactos de Soporte.

- Clasificación:

Pertenece a la categoría de documentos de incorporación y formación.

- Relación con Otros:

Se conecta con el manual de seguridad informática y los procedimientos de incorporación.

Documentos Derivados de la Ejecución Práctica:

Procedimientos y Herramientas de Detección de Riesgos:

- Descripción Funcional:

Facilita la identificación y evaluación proactiva de riesgos de seguridad informática.

- Estructura o Formato:

Procedimientos Detallados, Herramientas Utilizadas y Criterios de Evaluación.

- Clasificación:

Encaja en el área de gestión de riesgos y seguridad de la información.

- Relación con Otros:

Se vincula con el protocolo de respuesta a incidentes y los informes de seguimiento.

Informes de Seguimiento de Seguridad Informática:

- Descripción Funcional:

Proporciona información actualizada sobre el estado de seguridad informática.

- Estructura o Formato:

Resumen Ejecutivo, Métricas, Análisis de Tendencias y Acciones Correctivas.

- Clasificación:

En el ámbito de la supervisión continua y evaluación de controles de seguridad.

- Relación con Otros:

Está conectado con los informes de auditorías externas y el plan de formación en compliance.

Informes de Auditorías de Seguridad Informática:

- Descripción Funcional:

Evalúa la efectividad de los controles de seguridad implementados.

- Estructura o Formato:

Objetivos de Auditoría, Hallazgos, Recomendaciones y Planes de Acción Correctiva.

- Clasificación:

Perteneciente al ámbito de auditoría y evaluación de la seguridad.

- Relación con Otros:

Tiene relación con el manual de seguridad informática y los informes regulares para la administración.

Formularios de Incidentes de Seguridad y Modelos de Evidencia:

- Descripción Funcional:

Facilita la recopilación sistemática de información sobre incidentes y pruebas.

- Estructura o Formato:

Campos Detallados para Incidentes, Pruebas Recopiladas y Acciones Tomadas.

- Clasificación:

En el área de gestión de incidentes y evidencia forense.

- Relación con Otros:

Se conecta directamente con el protocolo de respuesta a incidentes y los informes de seguimiento.

Informes Regulares de Seguridad Informática para la Administración:

- Descripción Funcional:

Informa a los órganos de administración sobre el estado de la seguridad informática.

- Estructura o Formato:

Resumen Ejecutivo, Análisis de Riesgos, Incidentes Recientes y Medidas Recomendadas.

- Clasificación:

En la categoría de informes ejecutivos y de gestión.

- Relación con Otros:

Relacionado con los informes de auditorías externas y los planes de formación en compliance.

Políticas Específicas de Seguridad para Sistemas:

- Descripción Funcional:

Detalla prácticas seguras específicas para sistemas críticos.

- Estructura o Formato:

Configuración Segura de Sistemas, Acceso a Servidores y Medidas Específicas de Protección.

- Clasificación:

En el área de gestión de sistemas y seguridad.

- Relación con Otros:

Directamente conectado con el manual de seguridad informática y las políticas generales de seguridad.