INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 6

2 DE NOVIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado.

Para poder lograr establecer una cultura de la ciberseguridad en la empresa, es necesario que se establezca un plan para implementarla. En nuestro caso, la cultura de la ciberseguridad se realizará mediante un plan de concienciación.

1. Identificar necesidades.

2. Destacar debilidades.

Introducción

Desarrollar e integrar una cultura de seguridad dentro de nuestra organización es uno de los objetivos más complejos de alcanzar. En primer lugar porque su aplicación requiere de unos plazos de tiempo amplios y de acciones continuadas en el tiempo; en segundo lugar, y mucho más importante, porque hablamos de personas. Conseguir que nuestros empleados interioricen en sus quehaceres cotidianos una manera de trabajar que garantice que las cosas se hacen bien en materia de seguridad de la información no es una tarea sencilla.

La empresa para mantener un adecuado nivel de seguridad debe:

- REALIZAR ACCIONES DE FORMACIÓN EN SEGURIDAD PARA EMPLEADOS.

- ESTABLECER POLÍTICAS, NORMATIVAS Y PROCEDIMIENTOS DE SEGURIDAD.

- SUPERVISAR QUE SE CUMPLEN LAS BUENAS PRÁCTICAS EN SEGURIDAD.

- REALIZAR ACCIONES DE SENSIBILIZACIÓN Y CONCIENCIACIÓN EN SEGURIDAD PARA EMPLEADOS.

Identificar necesidades

REALIZAR ACCIONES DE FORMACIÓN EN SEGURIDAD PARA EMPLEADOS.

Es fundamental que seamos conscientes de la importancia de formar a nuestros empleados en materia de seguridad de la información para nuestros intereses como organización, y no sólo en materia de protección de datos personales, sino también desde el punto de vista de toda la información que trata la organización: datos de facturación, tarifas, márgenes, sistemas de producción, clientes, proveedores, acuerdos, etc.

Sin embargo, no todo el personal de una organización necesita el mismo tipo ni grado de formación en materia de seguridad. La formación que necesita el personal técnico que gestiona los servidores no debe ser la misma que reciba el usuario final que sólo dispone de acceso a una pequeña parte de la información corporativa.

<u>En el personal técnico:</u>

El personal técnico del Departamento de Informática es quien precisa más formación en materia de seguridad y con un mayor grado de especialización. Debemos poner a disposición

de los administradores de sistemas los recursos y mecanismos adecuados para formarse o autoformarse en aspectos relacionados con la seguridad de los sistemas y aplicaciones que dan soporte a los procesos de negocio de nuestra organización.

Se pueden destacar cosas como:

Los usuarios finales:

La seguridad hoy en día no se debe limitar sólo a los aspectos técnicos, sino que debe incorporar otros ámbitos como el organizativo y el legal, rebasando así las competencias del Departamento de Informática o sistemas.

Si nuestra empresa tiene como clientes a personas físicas resulta fundamental la formación en el ámbito de protección de datos de carácter personal, puesto que el nivel de riesgo asociado puede ser muy alto.

todo el personal de la organización con acceso a los sistemas de información corporativos debe recibir formación relacionada con buenas prácticas en materia de seguridad en su puesto de trabajo y en el desempeño de sus funciones:

ESTABLECER POLÍTICAS, NORMATIVAS Y PROCEDIMIENTOS DE SEGURIDAD.

Cuando se incorpora un nuevo empleado a la organización, es necesario que llevemos a cabo una serie de tareas relacionadas con el proceso de alta para que pueda empezar a desarrollar sus funciones:

- Tareas técnicas: alta del usuario en el dominio corporativo, asignación del ordenador personal, instalación del software que necesite, etc.

- Tareas administrativas: el nuevo empleado deberá firmar su contrato de trabajo y demás documentación relacionada con su alta laboral, documentación relacionada con el RGPD, el acuerdo de confidencialidad, y otras tareas como formación en temas de prevención de riesgos laborales, etc.

SUPERVISAR QUE SE CUMPLEN LAS BUENAS PRÁCTICAS EN SEGURIDAD.

La formación y la normalización de los protocolos de trabajo en nuestra empresa forman parte de los controles preventivos orientados a mejorar el nivel de seguridad de la organización. Una vez definido el marco de trabajo y trasladado a las partes afectadas, será necesario comprobar que efectivamente se está siguiendo y aplicando. Para ello, deberá existir un responsable de Seguridad encargado de velar por:

- La vigencia y correspondiente actualización de las normas y procedimientos definidos.

- La implantación de los mismos y su cumplimiento por parte de los empleados.

También dispondremos de mecanismos para comprobar que los empleados siguen los procedimientos definidos y que cumplen las normativas vigentes. Para ello realizaremos auditorías, ya sean internas o externas. Además podemos emplear herramientas de auditoría informática que registren las operaciones que realizan los usuarios en las aplicaciones y bases de datos corporativas, con objeto de garantizar la trazabilidad de esas operaciones.

REALIZAR ACCIONES DE SENSIBILIZACIÓN Y CONCIENCIACIÓN EN SEGURIDAD PARA EMPLEADOS.

Sea cual sea nuestro negocio, es importante que la cultura de la seguridad sea una de las bases de la filosofía de la empresa. Por este motivo, es fundamental que la Dirección se asegure de la implicación de todos los empleados.

Para conseguir esta implicación, es necesario emprender acciones de sensibilización y concienciación, necesarias para el mantenimiento de los niveles de seguridad adecuados. Si los empleados no se consideran parte fundamental de este proceso, el fracaso está garantizado, ya que ellos son los grandes protagonistas de esta historia.

Nuestro objetivo debe ser concienciarles sobre el papel que juegan en el mantenimiento de la seguridad de la información de la empresa.

Es necesario que los empleados conozcan los riesgos a los que están expuestos, para que sepan reaccionar correctamente ante posibles situaciones similares. Si no conocen estas amenazas, no podrán identificarlas ni protegerse frente a ellas. Algunos temas por los que se puede concienciar a los empleados es:

- Uso seguro de redes wifi.
- Uso seguro del correo electrónico.
- Prácticas de navegación segura.
- Identificación de virus y malware.
- Gestión de contraseñas.
- Clasificación de la información.
- Borrado seguro de la información.
- Uso de dispositivos USB.
- Seguridad en dispositivos móviles.
- Uso de programas de mensajería instantánea.
- Riesgos de las redes sociales.
- Técnicas de ingeniería social.