FUNDAMENTOS DE CIBERSEGURIDAD

Actividad de transferencia

Llego la hora de poner en práctica todo lo aprendido hasta ahora sobre la importancia de la ciberseguridad, las 10 Vs del Big Data, la seguridad de la información y la evaluación y tratamiento de los riesgos. Para lograrlo te propongo el siguiente ejercicio:

Imagina que empiezas a trabajar en una organización en la que la política de seguridad de la información todavía no existe. La organización busca ofrecer un servicio seguro y eficiente para la destrucción de documentos confidenciales. El objetivo de la empresa es ofrecer un servicio altamente flexible para satisfacer las necesidades del cliente y a su vez, ofrecer una seguridad de la información sin comparación para la total tranquilidad de sus clientes.

Recordemos que uno de los principales riesgos de la información en cualquier organización proviene de las personas dentro de cualquier proceso. En este orden de ideas, algunas amenazas pueden surgir de una mala práctica, un simple error humano o por inacción. Adicionalmente, la seguridad de la información es fundamental para el éxito de la empresa ya que gran parte de su trabajo consiste en recibir, analizar y almacenar información sensible sobre información crediticia de consumidores y empresas. Como consecuencia, es vital que la organización cuente con los controles adecuados para proteger sus sistemas de los cibercriminales y evitar que la su base de datos caiga en manos equivocadas, ya que existe un riesgo real de ser utilizada por los delincuentes para la suplantación de identidad. Por lo tanto, es imperativo que la organización pueda asegurar a sus clientes y al público en general que se toma en serio la seguridad de su información personal y para esta rigurosa tarea usted forma parte del equipo responsable.

La organización será auditada regularmente tanto por sus clientes como por otras partes interesadas. La organización anticipa que, en el futuro, este escrutinio de terceros no hará más que aumentar.

La rigurosa aplicación de las normas que elaboremos para esta organización garantizará que el personal el personal esté preparado para evitar y enfrentar todos los riesgos, además de cumplir con la legalidad.

Para cumplir satisfactoriamente con esta tarea asignada deberás:

1. Identificar las consecuencias de la filtración de información sensible.
2. Nombrar los tres elementos claves de la seguridad de la información.
3. Describir brevemente cómo debe elaborarse la política de seguridad según la norma ISO 27001.
4. Identificar algunos riesgos de la empresa y clasificar su prioridad en base a la escala Likert vista.

**Nota**: Si es necesario puede hacer suposiciones sobre el funcionamiento de su organización modelo. En estos casos, indique claramente las suposiciones que ha hecho.