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.

1. Consecuencias de la filtración de información sensible

La filtración de la información sensible puede tener varias consecuencias graves para una organización, especialmente una que maneja datos confidenciales como información crediticia:

- **Daño a la reputación:** La pérdida de confianza por parte de los clientes y el público en general puede ser devastadora. Una filtración puede hacer que los clientes se sientan vulnerables y opten por dejar de utilizar los servicios de la organización, afectando directamente su reputación y su posición en el mercado.
- **Impacto financiero:** Dependiendo de la magnitud de la filtración, la organización puede enfrentar multas regulatorias, costos legales y compensaciones a clientes afectados. Además, la pérdida de ingresos debido a la fuga de clientes es una consecuencia financiera directa.

- **Riesgo de suplantación de identidad:** los datos filtrados pueden ser utilizados por delincuentes para cometer fraudes de identidad, afectando tanto a los clientes en mayor medida como a la organización.

2. Elementos claves de la seguridad de la información

Tres de los elementos clave de la seguridad de la información son:

- **Confidencialidad:** asegurar que la información solo sea accesible para aquellos autorizados a tener acceso.
- **Integridad:** garantizar que la información sea precisa y completa y que no haya sido alterada de manera no autorizada.
- **Disponibilidad:** asegurar que la información esté disponible y accesible cuando sea necesario para los usuarios autorizados.

3. Elaboración de la política de seguridad según ISO 27001

La política de seguridad de la información según la norma ISO 27001 debe seguir estos pasos:

- **Contexto de la organización:** entender el contexto interno y externo que afecta a la seguridad de la información, incluyendo las necesidades y expectativas.
- **Liderazgo y compromiso:** compromiso de alta dirección para establecer una política de seguridad de la información y asegurar que sea compatible con los objetivos estratégicos de la organización.
- **Planificación:** definir un proceso sistemático para gestionar los riesgos de seguridad de la información, identificando amenazas, evaluando vulnerabilidades y estableciendo controles adecuados.
- **Soporte y operación:** implementación de controles y medidas de seguridad adecuadas, incluyendo recursos humanos, capacitación y concienciación.
- **Evaluación de desempeño y mejora:** establecimiento de indicadores de desempeño para monitorear y medir continuamente la eficacia de los controles de seguridad de la información, así como el compromiso con la mejora continua.

4. Riesgos de la empresa y clasificación por prioridad

Algunos riesgos potenciales para la organización de destrucción de documentos confidenciales podrían incluir:

- **Acceso no autorizado a documentos confidenciales:** prioridad alta, dado el impacto en la confidencialidad e integridad de la información.
- **Errores humanos en la gestión de documentos:** prioridad media, dado que podrían comprometer la integridad y disponibilidad de la información.

- **Ataques cibernéticos dirigidos a obtener información sensible: p**rioridad alta, debido al riesgo significativo para la confidencialidad y la integridad de los datos. Este es uno de los puntos más engañosos, dado que muchos negocios pequeños o medianos creen que los ataques cibernéticos se dan únicamente a empresas grandes y que por ello no invertirán en ciberseguridad; por ello, los ataques se dan más comúnmente a empresas medianas y pequeñas, por su baja seguridad en su información.