Registro de riesgos

Registro de riesgos

## Entorno operativo:

El banco está ubicado en una zona costera con bajos índices de criminalidad. Muchas personas y sistemas manejan los datos del banco: 100 empleados locales y 20 empleados remotos. La base de clientes del banco incluye 2000 cuentas individuales y 200 cuentas comerciales. Los servicios del banco son comercializados por un equipo deportivo profesional y diez empresas locales de la comunidad. Existen estrictas regulaciones financieras que exigen que el banco proteja sus datos y fondos, como tener suficiente efectivo disponible cada día para cumplir con los requisitos de la Reserva Federal.

| activos | Riesgos | Descripción | probabilidad | gravedad | Prioridad |
| --- | --- | --- | --- | --- | --- |
| fondos | Compromiso de correo empresarial | Un empleado es engañado para que comparta información confidencial | 2 | 3 | alta (6) |
|  | Base de datos de usuarios comprometida | Los datos de los clientes están mal cifrados. | 2 | 3 | alta (6) |
|  | Fuga de registros financieros | *Un servidor de base de datos de datos respaldados es de acceso público* | 2 | 3 | alta(6) |
|  | robo | La caja fuerte del banco está abierta. | 1 | 3 | baja (3) |
|  | Interrupción de la cadena de suministro | Retrasos en la entrega debido a desastres naturales. | 2 | 3 | alta (6) |

Notas

¿Cómo son posibles los eventos de seguridad considerando los riesgos que enfrenta el activo en su entorno operativo?

Al tener relativamente pocos empleados en el banco, es sencillo que reine un sentimiento de confianza y fiabilidad entre pares y clientes, recomendamos una fuerte capacitación sobre políticas de contraseñas y concientización sobre campañas de phishing, descarga de archivos maliciosos y sobre divulgación de datos, todo ello contemplado en la política de seguridad y prevención del Banco.

Con respecto al cifrado de datos sensibles, se recomienda reforzarlos.

Finalmente teniendo en cuenta la ubicación geográfica del banco, se recomienda que cuenten con un plan de contingencia ante algún evento cismático que involucre desastres naturales, teniendo en cuenta la infraestructura y demás elementos físicos que pudieran verse dañados o perjudicados: debe contemplarse esa probabilidad aunque sea mínima.

## Puntuación de los riesgos en funcion de su probabilidad

Teniendo en cuenta la fórmula : Probabilidad x impacto = Riesgo, se detalla en la tabla la probabilidad de que suceda un incidente de los detallados en la tabla.

Se opta por evaluar en baja, media y alta para mayor legibilidad

Se tuvieron en cuenta las siguientes cuestiones:

Una forma habitual de estimar la probabilidad del riesgo es determinar la frecuencia potencial de que se produzca:

¿Podría ocurrir el riesgo una vez al día?

¿Podría ocurrir el riesgo una vez al mes?

¿Podría ocurrir el riesgo una vez al año?

En este caso, el equipo está puntuando la probabilidad de un acontecimiento en una escala de 1 a 3:

1 representa un acontecimiento con una probabilidad baja de producirse.

2 representa un acontecimiento con una probabilidad moderada de ocurrir.

3 representa una alta probabilidad de que ocurra.

Al evaluar la gravedad de un riesgo, considere las consecuencias potenciales de que ese riesgo se produzca:

¿Cómo se vería afectada la empresa?

¿Cuál es el perjuicio financiero para la empresa y sus clientes?

¿Pueden verse afectadas operaciones o servicios importantes?

¿Se pueden infringir normativas?

¿Cuál es el daño a la reputación de la empresa?

Utilice la fila superior de la matriz de riesgos y considere el impacto potencial de cada riesgo. Estime una puntuación de gravedad para cada riesgo. A continuación, introduzca una puntuación (1-3 ) para cada riesgo en la columna de gravedad del registro:

1 (gravedad baja)

2 (gravedad moderada)

3 (gravedad alta )

### Glosario de referencia para interpretar la tabla

**Activo:** activo que corre el riesgo de sufrir daños, ser dañado o robado.

**Riesgo:** riesgo potencial para los sistemas de información y los datos de la organización.

**Descripción**: vulnerabilidad que podría provocar un incidente de seguridad.

**Probabilidad:** puntuación de 1 a 3 de las posibilidades de que se explote una vulnerabilidad. Un 1 significa que hay una probabilidad baja, un 2 significa que hay una probabilidad moderada y un 3 significa que hay una probabilidad alta.

**Gravedad:** puntuación de 1 a 3 del daño potencial que la amenaza causaría a la empresa. Un 1 significa un impacto de gravedad baja, un 2 significa un impacto de gravedad moderada y un 3 significa un impacto de gravedad alta.

Prioridad: con qué rapidez se debe abordar un riesgo para evitar el posible incidente. Utilice la siguiente fórmula para calcular la puntuación general: probabilidad x gravedad del impacto = riesgo

## Ejemplo de matriz de riesgo



|  | Bajo  1  1 | Moderado  2 | Catastrófico  3 |
| --- | --- | --- | --- |
| Cierto  3 | 3 | 6 | 9 |
| Probable  2 | 2 | 4 | 6 |
| Raro  1 | 1 | 2 | 3 |