INFORME DE ANÁLISIS DE RIESGO
SECCIÓN LABORAL
EMPRESA

Elaborado Por:

Equipo de Gestión de Seguridad de la Información

Introducción

En base al acuerdo 2-2021 anexo "Política de Seguridad de la Información de la EMPRESA" que establece que la información es un activo crítico, esencial y de gran valor para el desarrollo de las actividades de la institución, la Equipo de Gestión de Seguridad de la Información ha iniciado con el levantamiento de activos de información y análisis de riesgo de Sección Laboral de la EMPRESA.

Antecedentes

Actualmente el personal de la EMPRESA carece de conocimiento de los riesgos a los que están asociados los activos de información que están bajo su resguardo.

Objetivos

Proteger los activos de información de Sección Laboral de la EMPRESA mediante la implementación del Sistema de Gestión de Seguridad de la Información.

Identificar, mediante análisis los riesgos a los que están expuestos los activos informáticos y de información.

Metodología

La metodología utilizada para realizar el análisis de riesgo está basada en las normas internacionales ISO 31000 Gestión del riesgo e ISO 27001 Sistema de Gestión de Seguridad de la Información.

Para la implementación del Sistema de Gestión de Seguridad de la Información se debe Gestionar el Riesgo a los cuales están asociados los activos de información. Así pues, tomando como referencia lo expuesto anteriormente se realizan las siguientes actividades:

- Se inicia con una primera entrevista, en la cual se realiza la recolección de los activos informáticos y de información de las dependencias de la EMPRESA.
- La Equipo de Gestión de Seguridad de la Información realiza una serie de formularios, los cuales están asociados a los riesgos que se pueden materializar en los activos recolectados.
- Los Formularios son trasladados al contacto de la dependencia analizada para sus respectivas respuestas.
- La Equipo de Gestión de Seguridad de la Información procede a realizar el análisis de riesgo con la información proporcionada por la dependencia analizada.

- Se traslada el resultado del análisis realizado al jefe de la dependencia a través de un informe, en el que se indican los riesgos que representan mayor

relevancia para el desarrollo de sus funciones, así como propuestas para la disminución de estos.

- Posteriormente, la Equipo de Gestión de Seguridad de la Información deberá dar seguimiento realizando un nuevo análisis para determinar si los mismos han disminuido.

NIVELES DE RIESGO

El nivel de riesgo está calculado por el producto de la probabilidad (frecuencia con que ocurre un echo) por el impacto (nivel en el que se ve afectado el activo) de que un riesgo se llegue a materializar, la Equipo de Gestión de Seguridad de la Información realizó la clasificación de los niveles de riesgo a los que pueden estar asociados los activos de información en cuatro tipos que se representan por medio de un gráfico de calor, el cual se detalla de la siguiente manera:

NIVELES DE RIESGO	DESCRIPCIÓN
ACEPTABLE	Los ID de riesgo (número riesgo), que se encuentran en esta área tiene escasas posibilidades de materializarse, los activos se encuentran en un área confiable, se encuentran íntegros y disponibles, no obstante, estos deberán ser monitoreados constantemente y mantenerse en dicho nivel.
MODERADO	Los ID de riesgo (número riesgo), que se encuentran en esta área tiene mayor probabilidad que se materialicen en comparación de los que se encuentran en un nivel aceptable, por tal razón deben ser monitoreados para reducir el riesgo.
IMPORTANTE	Los ID de riesgo (número riesgo), que se encuentran en esta área están PRESENTES, por lo que es necesario implementar controles para mitigar, evitar o compartir el riesgo y reducir el nivel del riesgo.
INACEPTABLE	Los ID de riesgo (número riesgo), que se encuentran en esta área SON PRIORITARIOS, por lo que es necesario tomar medidas inmediatas por medio de la implementación de controles para mitigar, evitar o compartir el riesgo y reducir el nivel de riesgo.

***Los ID de Riesgo** son números asignados por la Equipo de Gestión de Seguridad de la Información a cada riesgo según al activo que corresponda.

Recolección de Información

Se tomó como muestra para las secciones la información recolectada sobre activos informáticos y activos de información en Sección de Familia y el Menor, proporcionado la información que se presenta a continuación:

Activos Informáticos:

- Sistema Informático de Expedientes de la EMPRESA (SIECC).
- INFILE Leyes
- Correo Electrónico Institucional.

Activos de Información:

- Proyectos Sentencia.
- Leyes Físicas.

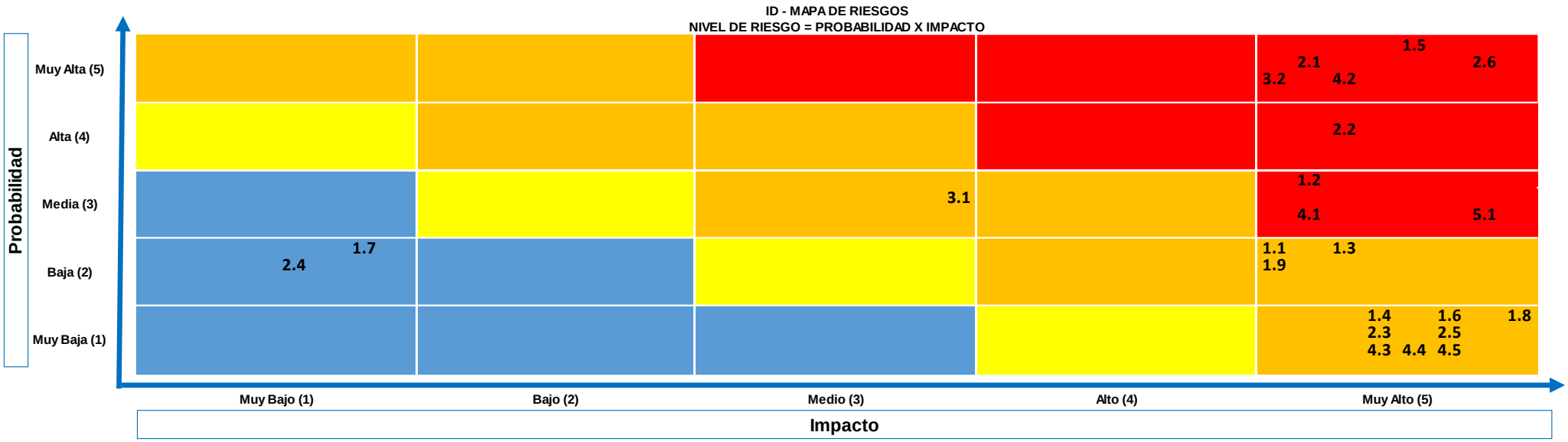
Análisis

Como resultado de la información recabada en los diferentes instrumentos (entrevistas, formularios), la Unidad de Gestión de Seguridad de Información de la EMPRESA clasificó los riesgos a los que están asociados los activos de información de la siguiente manera:

DEPENDENCIA: SECCIÓN LABORAL									
No.	Activo	ID Riesgo	Riesgo	Medición					
				Probabilidad de Ocurrencia		Impacto		Nivel de Riesgo	
1	Correo Institucional	1.1	Falla en el Acceso a Correo Institucional por problemas técnicos.	Baja	2	Muy Alto	5	10	Importante
		1.2	Pérdida y/o Robo de Credenciales por manejo de contraseña.	Media	3	Muy Alto	5	15	Inaceptable
		1.3	Pérdida y/o Robo de Credenciales por compartir Datos en Web.	Baja	2	Muy Alto	5	10	Importante
		1.4	Acceso o Manipulación de Información por compartir credenciales	Muy Baja	1	Muy Alto	5	5	Importante
		1.5	Pérdida Parcial y/o Total de Información por no realizar resguardo de información contenida en correo.	Muy Alta	5	Muy Alto	5	25	Inaceptable
		1.6	Fuga de Información por uso de correo personal para resguardar información de la institución	Muy Baja	1	Muy Alto	5	5	Importante
		1.7	Fuga de Información por Uso de Correo Institucional en Múltiples Dispositivos	Baja	2	Muy Bajo	1	2	Aceptable
		1.8	Acceso de Información por Terceros por compartir de forma errónea información vía correo electrónico	Muy Baja	1	Muy Alto	5	5	Importante
		1.9	Fraude Cibernético por Correo Electrónico	Baja	2	Muy Alto	5	10	Importante
2	Sistema Informático de Expedientes de la EMPRESA (SIECC)	2.1	Falla en el Acceso a SIECC por problemas técnicos.	Muy Alta	5	Muy Alto	5	25	Inaceptable
		2.2	Acceso no Autorizado a SIECC	Alta	4	Muy Alto	5	20	Inaceptable
		2.3	Acceso o Manipulación No Autorizado a la Información	Muy Baja	1	Muy Alto	5	5	Importante
		2.4	Fuga de Información por uso de SIECC en Múltiples Dispositivos	Baja	2	Muy Bajo	1	2	Aceptable
		2.5	Ingreso de información errónea	Muy Baja	1	Muy Alto	5	5	Importante
		2.6	Retraso en operación por Ausencia de Control de Calidad en Digitalización de Documentos	Muy Alta	5	Muy Alto	5	25	Inaceptable

3	INFILE	3.1	Fallas en el Acceso a Sistema INFILE	Media	3	Medio	3	9	Importante
		3.2	Uso de Credenciales por Terceros no Autorizados	Muy Alta	5	Muy Alto	5	25	Inaceptable
4	Documentos Digitales	4.1	Acceso No Autorizado a Equipos por manejo de contraseña.	Media	3	Muy Alto	5	15	Inaceptable
		4.2	Pérdida Parcial y/o Total de Información contenida en equipo de cómputo por no realizar resguardo de información.	Muy Alta	5	Muy Alto	5	25	Inaceptable
		4.3	Acceso no Autorizado a la Información por dejar desatendido equipo de cómputo	Muy Baja	1	Muy Alto	5	5	Importante
		4.4	Pérdida Parcial y/o Total de Información contenida en equipo de cómputo por compartir credenciales.	Muy Baja	1	Muy Alto	5	5	Importante
		4.5	Pérdida Parcial y/o Total de Información por desastres naturales	Muy Baja	1	Muy Alto	5	5	Importante
5	Leyes	5.1	Deterioro y/o Pérdida de Publicaciones por resguardo inadecuado.	Media	3	Muy Alto	5	15	Inaceptable

Los resultados obtenidos del análisis de riesgo se muestran en el siguiente Mapa de Riesgo o Mapa de Calor.



Dentro del Mapa de Riesgo o Mapa de Calor se encuentran distribuidos los riesgos a los que están asociados los activos de información por medio del ID Riesgo. Los colores representan el Nivel del Riesgo en que se encuentra cada uno de los mismos.

Resultados

Los riesgos asociados a los activos informáticos y de información que se encuentran en una zona **INACEPTABLE** dentro del Mapa de Calor son:

- **Correo Electrónico**

    - **Pérdida y/o Robo de Credenciales por manejo de contraseña (1.2).** Se asoció este nivel de riesgo por los siguientes factores:
        - Utilización de una contraseña para el ingreso al Correo Electrónico que no cumple con las características de una contraseña segura.
        - Utilización de la misma contraseña por periodos prolongados.

    - **Pérdida Parcial y/o Total de Información por no realizar resguardo de información contenida en correo (1.5).** Se asoció este nivel de riesgo por los siguientes factores:
        - No realizar resguardo de Información.
        - Desconocimiento de cómo realizar el resguardo de información del Correo Electrónico.
        - Fallas del proveedor de Servicio de Correo electrónico
        - Eliminación de Correos relevantes para el desarrollo de las funciones sin intención.

- **Sistema Informático de Expedientes de la EMPRESA.**

    - **Fallas en el Acceso a SIECC por problemas técnicos. (2.1).** Se asoció este nivel de riesgo por los siguientes factores:
        - Fallas en la red interna de la EMPRESA.
        - Fallas en el sistema (SIECC).

    - **Acceso no Autorizado a SIECC. (2.2).** Se asoció este nivel de riesgo por los siguientes factores:
        - Utilización de una contraseña para el ingreso al SIECC que no cumple con las características de una contraseña segura.
        - Utilización de la misma contraseña por periodos prolongados.

    - **Retraso en operaciones por Ausencia de Control de Calidad en Digitalización de Documentos. (2.6).** Se asoció este nivel de riesgo por los siguientes factores:
        - No contar con un proceso o procedimiento en el área de escaneo para verificar que la información escaneada sea legible y completa.

- Falta de procedimiento en área de recepción para verificar que la información recibida en formato digital este completa y legible.

- **INFILE Leyes**

  - **Uso de credenciales por Terceros no Autorizados (3.2).** Se asoció este nivel de riesgo por los siguientes factores:
    - No todos los colaboradores del área cuentan con credenciales para acceder al Sistema.
    - No utilizar el correo institucional como usuario para el acceso al Sistema.

- **Documentos Digitales (Notificaciones de Autos y Sentencias, elaboración de ejecutorias).**

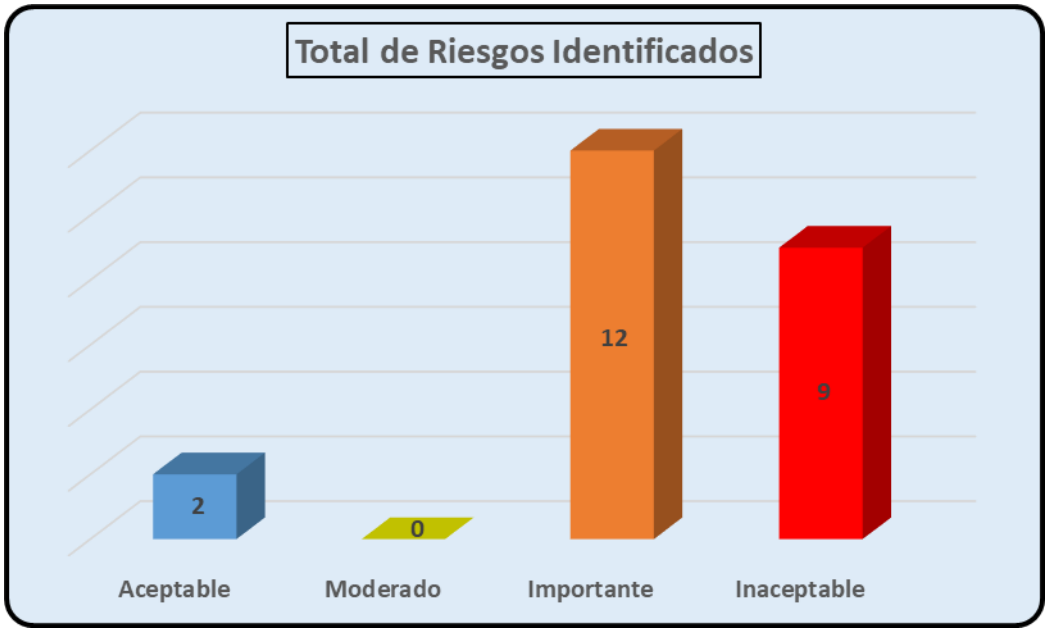
  - **Acceso No Autorizado a Equipo por manejo de contraseña (4.1).** Se asoció este nivel de riesgo por los siguientes factores:
    - Utilización de una contraseña para el ingreso al equipo de cómputo que no cumple con las características de una contraseña segura.
    - Utilización de la misma contraseña por periodos prolongados.

  - **Pérdida parcial y/o Total de Información contenida en equipo de cómputo por no resguardar la información (4.2).** Se asoció este nivel de riesgo por los siguientes factores:
    - Los equipos de cómputo son susceptibles a averías por diferentes razones, por ello es necesario que la información que se resguarda dentro de los mismos cuente con una copia de seguridad.
    - No realizar una copia de seguridad.
    - El no contar con una copia de seguridad pone en riesgo la continuidad de las operaciones.

- **Documentos Físicos (Leyes).**

  - **Deterioro y/o Pérdida de Leyes por resguardo inadecuado (5.1).** Se asoció este nivel de riesgo por los siguientes factores:
    - Dejar las leyes utilizadas para el desarrollo de funciones al alcance de terceras personas.
    - No contar con un área establecida para el resguardo de la información física (Leyes).

A continuación, se muestra un gráfico en el cual representa los niveles de riesgo en que se encuentran los riesgos identificados en el análisis realizado por la Equipo de Gestión de Seguridad de la Información.



El objetivo es que todos los riesgos asociados a los activos de Sección Laboral estén en un nivel **Aceptable** (representado en color azul), dando inicio con el tratamiento a los que se encuentran en un nivel **INACEPTABLE** (representado en color rojo).

Los riesgos identificados afectan en una u otra medida los pilares de la información Confidencialidad (C), Integridad (I), Disponibilidad (D), en la siguiente tabla se da una representación porcentual de cómo afectaría a los activos si los riesgos que se encuentran en el área **INACEPTABLE** se llagaran a materializar.

El Nivel de Riesgo puede tomar los valores de 1 a 25 como resultado del producto de la probabilidad o frecuencia con que se realiza una acción (representada por los números de 1 – 5) por el impacto que genera la misma para el desarrollo de nuestras actividades (representado por los números del 1 – 5). Para realizar el cálculo del porcentaje se toma en consideración el Nivel de Riesgo, siendo 1 el nivel más bajo, equivalente al 100% de cumplimiento con los pilares asociados al riesgo y 25 el nivel más alto, equivalente al 0% de cumplimiento con los pilares asociados al riesgo.

ID Riesgo	Riesgo	Nivel de Riesgo	Porcentaje		
			C	I	D
1.2	Pérdida y/o Robo de Credenciales por manejo de contraseña.	15	42%	42%	42%
1.5	Pérdida Parcial y/o Total de Información por no realizar resguardo de información contenida en correo.	25			0%
2.1	Falla en el Acceso a SIECC por problemas técnicos.	25			0%
2.2	Acceso no Autorizado a SIECC	20	21%	21%	21%
2.6	Retraso en operación por Ausencia de Control de Calidad en Digitalización de Documentos	25	0%	0%	
3.2	Uso de Credenciales por Terceros no Autorizados	25	0%		0%
4.1	Acceso No Autorizado a Equipos por manejo de contraseña.	15	42%	42%	42%
4.2	Pérdida Parcial y/o Total de Información contenida en equipo de cómputo por no realizar resguardo de información.	25			0%
5.1	Deterioro y/o Pérdida de Leyes por resguardo inadecuado.	15			42%

Tomando de referencia la tabla anterior podemos dar una interpretación de los riesgos asociados a los pilares de la información tomando como base el Nivel de Riesgo de la siguiente forma:

- ID 1.2 afecta los tres pilares de la información, por lo cual se tendría 42% de cumplimiento. Poniendo en riesgo la información del correo electrónico de la Institución por manejo de contraseña.
- ID 1.5 afecta la Disponibilidad, por lo cual se tendría 0% de cumplimiento. Poniendo en riesgo la información contenida en el correo electrónico de la Institución por no realizar copias de seguridad.
- ID 2.1 afecta la Disponibilidad, por lo cual se tendría un 0% de cumplimiento. Poniendo en riesgo el acceso al Sistema Informático de Expedientes de la EMPRESA por fallas técnicas.
- ID 2.2 afecta los tres pilares de la información, por lo cual se tendrá un 21% de cumplimiento. Poniendo en riesgo la información resguardada en el Sistema Informático de Expedientes de la EMPRESA, por la utilización de una contraseña débil para el ingreso al sistema y utilizar la misma por periodos prolongados.

- ID 2.6 afecta la Confidencialidad e Integridad, por lo cual se tendría un 0% de cumplimiento. Poniendo en riesgo el tiempo de ejecución de las tareas, por elegibilidad o estar incompleta la información.
- ID 3.2 afecta la Confidencialidad y Disponibilidad, por lo cual se tendría un 0% de cumplimiento. Poniendo en riesgo el acceso al sistema INFILE por no estar asociado al correo institucional.
- ID 4.1 afecta los tres pilares, por lo cual se tendría un 42% de cumplimiento. Poniendo en riesgo la información resguardada en el equipo de cómputo por manejo de contraseña.
- ID 4.2 afecta la Disponibilidad, por lo cual se tendría un 0% de cumplimiento. Poniendo en riesgo la información resguardada en equipo de cómputo por no realizar resguardo de esta.
- ID 5.1 afecta la Disponibilidad, por lo cual se tendría un 42% de cumplimiento. Poniendo en riesgo las leyes que se encuentran en forma física por no resguardar las mismas de forma apropiada.

Conclusiones

- Del total de riesgos analizados el 39% se encuentra en un nivel INACEPTABLE y un 52% en un nivel IMPORTANTE, lo que implica tomar acciones para disminuir estos porcentajes por medio de estrategias y acciones para su mitigación. Para esto, se dará inicio con la propuesta de mitigación, reducción o transferencia de los que se encuentran en un nivel INACEPTABLE.
- A pesar de que un 0% se encuentran en un nivel MODERADO y un 9% en un nivel ACEPTABLE, estos deben ser monitoreados y controlados de una forma constante para que no suban a los niveles superiores.
- La materialización de los riesgos pone en peligro los tres pilares de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad) por lo que es importante darle el tratamiento apropiado a los mismos, y de esta manera garantizar la continuidad del negocio y la seguridad de la información.

Recomendación

- Cuando se menciona el tema de riesgo, por lo general, lo primero es asociarlo con algo malo, sin embargo, debe de ser visto como oportunidades de mejoras. La Equipo de Gestión de Seguridad de la Información ha elaborado un documento guía en el cual se proponen los planes de mitigación y planes de contingencia para los riesgos identificados en Sección Laboral, por ello se recomienda que los mismos sean tomados en cuenta a fin de evitar la materialización de los riesgos identificados.