RECOMENDACIONES PARA MITIGACIÓN DEL RIESGO
SECCIÓN LABORAL
EMPRESA

Elaborado Por:

Equipo de Gestión de Seguridad de la Información

.

Introducción

El Sistema de Gestión de Seguridad de la Información (SGSI) es la generación e implementación de estrategias para el tratamiento de los riesgos de los Activos Informáticos y Activos de Información, con la finalidad de resguardar, proteger, asegurar y garantizar la confidencialidad, integridad y disponibilidad.

Se presentan las siguientes **Cédulas de Riesgo** en las cuales se presentan los aspectos relevantes relacionados con el análisis realizado por la Equipo de Gestión de Seguridad de la Información, conteniendo las mismas:

- **Identificación del activo:** Nombre del o los activos relacionados con el riesgo.
- **Riesgo asociado al activo:** Nombre del riesgo identificado.
- **ID Riesgo:** Número asignado por la Equipo de Gestión de Seguridad de la Información a cada riesgo según el activo que corresponda.
- **Identificación del Riesgo:** listado de las posibles causas o fuentes del riesgo.
- **Análisis del riesgo:** se presenta un resumen del análisis realizado, así, como listar las consecuencias que se generarían al materializarse el mismo.
- **Plan de mitigación:** Desarrollo de estrategias para la reducción de probabilidad o impacto de riesgo.
- **Plan de contingencia:** Desarrollo de estrategias para saber cómo actuar ante una posible eventualidad.

Las Cédulas de Riesgo serán discutidas por Sección Laboral en conjunto con la Equipo de Gestión de Seguridad de la Información, para el desarrollo e implementación de estas.

Objetivo

El objetivo del desarrollo de las Cédulas de Riesgo es proponer proyectos para reducir la exposición al riesgo y llevar, los que se encuentran en un Nivel INACEPTABLE a un Nivel ACEPTABLE. Dándole el tratamiento adecuado a los activos informáticos y de información de Sección Laboral de la EMPRESA.

Activo:	Correo Institucional	**Cédula de Riesgo**
Riesgo:	Pérdida y/o Robo de Credenciales por manejo de contraseña.	**ID Riesgo: No. 1.2**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* Utilización de una contraseña considerada débil para el acceso a Correo Institucional. * Utilización de la misma contraseña por periodos prolongados.	
ANÁLISIS DEL RIESGO		
Probabilidad 3 Media	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 15 INACEPTABLE
Consecuencias	* Acceso a Correo Institucional por terceras personas. * Conocimiento de información resguardada en Correo Institucional.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Implementación Norma o Procedimiento de creación y uso de contraseña por parte de la dependencia.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal	
PLAN DE CONTINGENCIA		
Desencadenante	* CONOCIMIENTO DE INFORMACIÓN CONTENIDA EN CORREO INSTITUCIONAL POR TERCERAS PERSONAS.	
Acción(es)	* Implementación de Norma o Procedimiento por parte de la Dirección de Tecnologías de Información para creación y uso de contraseña segura dentro del Correo Institucional.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Apoyo de la Dirección de Tecnologías de la Información	

Activo:	Correo Institucional	**Cédula de Riesgo**
Riesgo:	Pérdida Parcial y/o Total de Información por no realizar resguardo de información contenida en correo.	**ID Riesgo: No. 1.5**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* Fallas del proveedor de servicios de Correo Electrónico. * Desconocimiento de cómo realizar resguardo de información o backup contenida en Correo Institucional.	
ANÁLISIS DEL RIESGO		
Probabilidad 5 Muy Alta	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 25 INACEPTABLE
Consecuencias	* Pérdida de información contenida en Correo Institucional. * Retraso en el desarrollo de funciones por no tener disponibilidad de la información contenida en Correo.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Implementación procedimiento para resguardo de la información o backup de Correo Institucional por parte de la dependencia.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal	
PLAN DE CONTINGENCIA		
Desencadenante	* PÉRDIDA DE INFORMACIÓN CONTENIDA EN CORREO INSTITUCIONAL	
Acción(es)	* Implementación de procedimiento por parte de la Dirección de Tecnologías de Información para realización de resguardo o backup de información en Correo Institucional.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Servidores de backup. * Financiero. * Personal. * Apoyo de la Dirección de Tecnologías de la Información	

Activo:	Sistema Informático de Expedientes de la EMPRESA - SIECC-		**Cédula de Riesgo**
Riesgo:	Falla en el Acceso a SIECC por problemas técnicos.		**ID Riesgo: No. 2.1**
IDENTIFICACIÓN DEL RIESGO			
¿Cuáles son las causas o fuentes del riesgo?	* Fallas en la red interna de la EMPRESA. * Fallo en el sistema.		
ANÁLISIS DEL RIESGO			
Probabilidad 5 Muy Alta	**Impacto** 5 Muy Alto		**Nivel de Riesgo** 25 INACEPTABLE
Consecuencias	* Retraso en operaciones por falta de acceso.		
Controles Existentes	* NO EXISTE CONTROL		
PLAN DE MITIGACIÓN			
Acción	Trasladar: * La Dirección de Tecnologías de Información debe realizar un plan de monitoreo de red.		
Fecha Inicial	15/6/2022	**Fecha Final**	31/12/2022
Recursos	* Software monitoreo de red. * Personal. * Financiero.		
PLAN DE CONTINGENCIA			
Desencadenante	* PÉRDIDA DE CONECTIVIDAD A SIECC / RETRASO EN OPERACIONES		
Acción(es)	* La Dirección de Tecnologías de Información debe realizar una programación para verificación y solución de problemas en el SIECC.		
Fecha Inicial	15/6/2022	**Fecha Final**	31/12/2022
Recursos	* Personal de la Dirección de Tecnologías de Información. * Financiero.		

Activo:	Sistema Informático de Expedientes de la EMPRESA - SIECC-	**Cédula de Riesgo**
Riesgo:	Acceso no Autorizado a SIECC	**ID Riesgo: No. 2.2**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* Utilización de contraseña débil para acceder al SIECC. * Utilización de la misma contraseña por periodos prolongados.	
ANÁLISIS DEL RIESGO		
Probabilidad 4 Alta	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 20 INACEPTABLE
Consecuencias	* Acceso y utilización del Sistema por terceras personas. * Conocimiento de información administrada en el SIECC. * Eliminación de información. * Reproceso de información.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Creación de Norma de Contraseña Segura y Periodicidad.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	
PLAN DE CONTINGENCIA		
Desencadenante	* CONOCIMIENTO DE INFORMACIÓN ADMINISTRADA EN SIECC POR TERCERAS PERSONAS - PÉRDIDA DE INFORMACIÓN	
Acción(es)	* Implementación de cambio periódico de contraseña y contraseña segura dentro del Sistema Informático de Expedientes de la EMPRESA por medio de la Dirección de Tecnologías de Información.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal Dirección de Tecnologías de Información. * Servidores para resguardo de información. * Financiero.	

Activo:	Sistema Informático de Expedientes de la EMPRESA - SIECC-	**Cédula de Riesgo**
Riesgo:	Retraso en operación por Ausencia de Control de Calidad en Digitalización de Documentos	**ID Riesgo: No. 2.6**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* No se verifica que la información escanea este completa y legible. * No se verifica que la información recibida en formato digital este completa y legible antes de cargarla al sistema.	
ANÁLISIS DEL RIESGO		
Probabilidad 5 Muy Alta	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 25 INACEPTABLE
Consecuencias	* Retraso en los tiempos de operaciones.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Trasladar: * Reestructuración del área de Digitalización para implementación de control de calidad.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	
PLAN DE CONTINGENCIA		
Desencadenante	* RETRASO EN OPERACIONES	
Acción(es)	* La Secretaria General deberá de implementar procedimientos para la Digitalización y Verificación de Documentos.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	

Activo:	INFILE	**Cédula de Riesgo**
Riesgo:	Uso de Credenciales por Terceros no Autorizados	**ID Riesgo: No. 3.2**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* No todos los usuarios cuentan con credenciales para el acceso. * No utilizar el correo institucional como usuario del sistema.	
ANÁLISIS DEL RIESGO		
Probabilidad 5 Muy Alta	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 25 INACEPTABLE
Consecuencias	* Acceso a sistemas por usuarios sin autorización.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Establecer una Norma o procedimiento para que cada usuario del área cuente con credencial para acceder al sistema.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	
PLAN DE CONTINGENCIA		
Desencadenante	* ACCESO A SISTEMA POR TERCERAS PERSONAS.	
Acción(es)	* Establecer un proceso por el encargado de gestionar las credenciales para los colaboradores del área para que el mismo está asociado al Correo Electrónico Institucional.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	

Activo:	Documentos Digitales (Proyectos).	**Cédula de Riesgo**
Riesgo:	Acceso No Autorizado a Equipos por manejo de contraseña.	**ID Riesgo: No. 4.1**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* Utilización de una contraseña, que no cumple con los criterios de contraseña segura. * Utilización de la misma contraseña por periodos prolongados.	
ANÁLISIS DEL RIESGO		
Probabilidad 3 Media	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 15 INACEPTABLE
Consecuencias	* Acceso a la información contenida en equipo de cómputo por terceras personas. * Borrado de información sin autorización. * Aumento de carga laboral por pérdida de información.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Implementación de Norma de Creación y uso de contraseña.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	
PLAN DE CONTINGENCIA		
Desencadenante	* ACCESO Y/O PÉRDIDA DE LA INFORMACIÓN CONTENIDA EN EL EQUIPO DE CÓMPUTO	
Acción(es)	* La Dirección de Tecnologías de Información implementara la utilización de contraseña segura para el ingreso al equipo de cómputo y cambio periódico de la misma.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal * Apoyo de la Dirección de Tecnologías de Información. * Apoyo del área de Servicios Generales * Financiero.	

Activo:	Documentos Digitales (Proyectos).	**Cédula de Riesgo**
Riesgo:	Pérdida Parcial y/o Total de Información contenida en equipo de cómputo por no realizar resguardo de información.	**ID Riesgo: No. 4.2**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* Desconocimiento de cómo realizar resguardo de información o backup. * Fallas en equipo de cómputo.	
ANÁLISIS DEL RIESGO		
Probabilidad 5 Muy Alta	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 25 INACEPTABLE
Consecuencias	* Pérdida por indisponibilidad de Información. * Reproceso de información. * Aumento de carga laboral por pérdida de información	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Implementación de procedimiento de resguardo de información digital. * Priorizar la información a resguardar.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Servidor para resguardo de información. * Financiero.	
PLAN DE CONTINGENCIA		
Desencadenante	PÉRDIDA DE LA INFORMACIÓN CONTENIDA EN EL EQUIPO DE CÓMPUTO	
Acción(es)	* Adquisición de software para recuperación de información. * Procedimiento para recuperación de información por medio de software.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal Dirección de Tecnologías de Información. * Software para recuperación de información. * Financiero.	

Activo:	Documentos Físicos (Leyes)	**Cédula de Riesgo**
Riesgo:	Deterioro y/o Pérdida de Leyes por resguardo inadecuado.	**ID Riesgo: No. 5.1**
IDENTIFICACIÓN DEL RIESGO		
¿Cuáles son las causas o fuentes del riesgo?	* Acceso no restringido a área. * Las Leyes se dejan al alcance de terceras personas. * No contar con un espacio para el resguardo de la información física.	
ANÁLISIS DEL RIESGO		
Probabilidad 3 Media	**Impacto** 5 Muy Alto	**Nivel de Riesgo** 15 INACEPTABLE
Consecuencias	* Retraso en las operaciones.	
Controles Existentes	* NO EXISTE CONTROL	
PLAN DE MITIGACIÓN		
Acción	Reducir: * Creación e Implementación de procedimiento de resguardo de información física dentro del área. * Creación e Implementación de acceso a área.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	
PLAN DE CONTINGENCIA		
Desencadenante	* PÉRDIDA O DETERIORO DE DOCUMENTOS FÍSICOS.	
Acción(es)	* Implementación de Política de escritorio y pantalla limpia.	
Fecha Inicial	15/6/2022	**Fecha Final** 31/12/2022
Recursos	* Personal. * Financiero.	