

Universidad Mariano Gálvez

Sede de Villa Nueva

Proyecto de Graduación 2



## Manual Técnico

Carlos Eduardo Galindo Miranda	5190-19-5184
Julio Estiven Dubon Morales	5190-19-6679
Mildred Madai Lima Barrios	5190-18-2440
Manuel Eduardo Ordoñez Silva	5190-19-4050
Carlos Rodolfo Bendfeldt Samayoa	5190-18-1748

Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4		Evelyn Lobos		
HECHO POR:		REVISADO POR:	APROBADO POR:	
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

INTRODUCCION:

La presente auditoría tiene como objetivo evaluar la implementación de las tecnologías de seguridad en Royal Services S.A., específicamente el firewall pfSense, el directorio activo Sentyal y el SIEM AlienVault. Estas tecnologías desempeñan un papel fundamental en la protección de la infraestructura tecnológica y la seguridad de la información de la empresa. El presente informe detalla los riesgos identificados, proporciona soluciones y concluye con recomendaciones para garantizar la efectividad de estas tecnologías de seguridad.

OBJETIVO GENERAL:

Evaluar la implementación y configuración de las tecnologías de seguridad, incluyendo el firewall pfSense, el directorio activo Sentyal y el SIEM AlienVault, con un enfoque en la protección de la infraestructura tecnológica y la seguridad de la información en Royal Services S.A.

ALCANCE:

La auditoría se centrará en evaluar la seguridad de la información en el sector BPO de Royal Services S.A., incluyendo la revisión de estándares, gestión de riesgos, plan de continuidad del negocio y capacitación del personal.

Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4		Evelyn Lobos		
HECHO POR:		REVISADO POR:	APROBADO POR:	
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

- Firewall pfSense: Se evaluará la configuración del firewall pfSense para garantizar la protección de la red y la detección de amenazas.
- Directorio Activo Sentyal: Se revisará la implementación del directorio activo Sentyal para asegurar el control y gestión eficaz de las identidades de usuario y el acceso a los recursos.
- SIEM AlienVault: Se evaluará la configuración y utilización del SIEM AlienVault para la detección y respuesta a amenazas en la red.

PRESUNCIÓN DE RIESGOS

- Accesos no autorizados a la información.
- Falta de un plan de continuidad del negocio.
- Cambios tecnológicos no gestionados.
- Amenazas cibernéticas avanzadas.
- Vulnerabilidades de seguridad en la infraestructura.
- Falta de capacitación del personal.
- Acceso no autorizado a datos confidenciales.

Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4	Evelyn Lobos			
HECHO POR:	REVISADO POR:	APROBADO POR:		
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

	<ul style="list-style-type: none"><li>• Pérdida de datos por fallo en la copia de seguridad.</li><li>• Escalada de privilegios internos.</li><li>• Suplantación de identidad (Phishing).</li><li>• Cumplimiento regulatorio inadecuado.</li><li>• Riesgo de desastres naturales.</li><li>• Configuraciones incorrectas o inadecuadas del firewall pueden exponer la red a amenazas no deseadas.</li><li>• Fallas en la gestión de accesos y permisos pueden resultar en accesos no autorizados a recursos críticos.</li><li>• La falta de un sistema eficiente de monitoreo y respuesta a amenazas puede llevar a una detección deficiente de incidentes de seguridad.</li></ul> <p><u>PROGRAMA DE TRABAJO A DESARROLLAR</u></p> <ul style="list-style-type: none"><li>• Validar la existencia y efectividad de un plan de continuidad del negocio.</li><li>• Revisar la gestión de cambios tecnológicos.</li><li>• Evaluar el nivel de capacitación del personal en seguridad de la información.</li></ul>		
--	---	--	--

Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4		Evelyn Lobos		
HECHO POR:		REVISADO POR:	APROBADO POR:	
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

	<ul style="list-style-type: none"><li>Realizar pruebas de seguridad en la infraestructura tecnológica.</li><li>Revisar el cumplimiento de regulaciones de seguridad específicas del sector financiero.</li></ul> <p><b>Evaluación de Configuración del Firewall pfSense:</b></p> <ul style="list-style-type: none"><li>Verificar la configuración del firewall pfSense para asegurar que las políticas de seguridad sean adecuadas y efectivas.</li><li>Identificar posibles vulnerabilidades y recomendaciones para mejoras.</li></ul> <p><b>Revisión del Directorio Activo Sentyal:</b></p> <ul style="list-style-type: none"><li>Evaluar la configuración del directorio activo Sentyal en términos de autenticación, autorización y control de acceso.</li><li>Revisar la implementación de políticas de contraseñas y políticas de seguridad de cuentas.</li></ul> <p><b>Análisis del SIEM AlienVault:</b></p> <ul style="list-style-type: none"><li>Evaluar la implementación del SIEM AlienVault para garantizar la detección y respuesta efectiva a eventos de seguridad.</li><li>Verificar que las alertas y notificaciones estén configuradas de manera apropiada.</li></ul> <p><b>Integración de Tecnologías de Seguridad:</b></p> <ul style="list-style-type: none"><li>Evaluar la integración de estas tecnologías de seguridad para garantizar la visibilidad y la eficacia en la detección y respuesta a amenazas.</li></ul> <p><b>Verificación de Registro y Auditoría:</b></p>		
--	---	--	--

Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4		Evelyn Lobos		
HECHO POR:		REVISADO POR:	APROBADO POR:	
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

- Revisar la capacidad de registro y auditoría de las tecnologías de seguridad para garantizar la trazabilidad de eventos de seguridad.

Políticas y Procedimientos:

Revisar las políticas y procedimientos de seguridad de la información de la empresa para evaluar su aplicabilidad, claridad y actualización.  
Verificar que los empleados estén al tanto de estas políticas y las sigan adecuadamente.

Evaluación de Controles de Acceso:

Realizar una revisión detallada de los controles de acceso a sistemas y datos, incluyendo la autenticación de dos factores, gestión de contraseñas, control de privilegios y sistemas de registro de acceso.

Gestión de Incidentes de Seguridad:

Evaluar la capacidad de la empresa para detectar, informar y responder a incidentes de seguridad.  
Realizar simulacros de incidentes para evaluar la respuesta y la comunicación interna y externa.

Protección de Datos Confidenciales:

Revisar las medidas de protección de datos, incluyendo la encriptación de datos sensibles, políticas de retención de datos y la protección de datos en tránsito y en reposo.

Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4		Evelyn Lobos		
HECHO POR:		REVISADO POR:	APROBADO POR:	
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

Evaluación de Proveedores y Terceros:

Evaluar la seguridad de los proveedores y terceros que tienen acceso a datos de la empresa.  
Revisar acuerdos de seguridad, evaluación de riesgos y asegurarse de que estos terceros cumplan con los estándares de seguridad necesarios.

Monitoreo Continuo:

Implementar soluciones de monitoreo continuo de seguridad para detectar y responder de manera proactiva a amenazas y actividades sospechosas en tiempo real.

Auditoría de Código y Aplicaciones:

Realizar auditorías de seguridad de aplicaciones y código fuente para identificar vulnerabilidades, como inyección de SQL, cross-site scripting (XSS) y otros problemas de seguridad en el software utilizado.

Gestión de Riesgos:

Realizar una evaluación más profunda de la gestión de riesgos de seguridad de la información, incluyendo la

Auditoría Interna Corporativa	<b>PROGRAMACIÓN</b> <b>AUDITORÍA DE SISTEMAS</b>		Código:	
			Fecha:	13/10/23
			Edición	
Grupo 4	Evelyn Lobos			
HECHO POR:	REVISADO POR:	APROBADO POR:		
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:		HECHO POR:	FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

identificación de activos críticos, análisis de riesgos y el desarrollo de un plan de tratamiento de riesgos.

### Pruebas de Ingeniería Social:

Realizar pruebas de ingeniería social para evaluar la concienciación y preparación del personal en la identificación y mitigación de amenazas de ingeniería social.

### Evaluación de Dispositivos Móviles:

Si la empresa utiliza dispositivos móviles, realizar una auditoría de seguridad específica en dispositivos móviles, incluyendo políticas de seguridad para dispositivos móviles y controles de acceso.

### Educación Continua:

Implementar programas de educación continua en seguridad de la información para mantener al personal actualizado sobre las últimas amenazas y mejores prácticas.

### Análisis de Redes:

Realizar un análisis de la topología de red y evaluar la seguridad de la infraestructura de red, incluyendo la segmentación y la protección contra intrusiones.



Auditoría Interna Corporativa	PROGRAMACIÓN		Código:	
	AUDITORÍA DE SISTEMAS		Fecha:	13/10/23
			Edición	
Grupo 4	Evelyn Lobos			
HECHO POR:	REVISADO POR:		APROBADO POR:	
NOMBRE DE LA EMPRESA AUDITADA				
PROCESO:	RECURSOS HUMANOS	REF. PT		
SUBPROCESO:	HECHO POR:		FECHA:	
ÁREA:	Gerencia de Recursos Humanos	REVISADO POR:	FECHA:	
DESCRIPCIÓN:				
Evaluar				
PROCEDIMIENTO			Responsable	Ref.

	<p><u>Pruebas de Resiliencia:</u></p> <p>Realizar pruebas de resiliencia para evaluar la capacidad de la empresa para recuperarse de incidentes de seguridad, como ataques de ransomware o desastres naturales.</p>		
--	---	--	--