	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Prevención de Fuga de Datos (DLP)
	Código:	PECRSI17

CONTROL DE CAMBIOS

Cambio en Formato a partir del PGCRC02 Elaboración de información Documentada
Organización de la información

1. OBJETIVO

Dar a conocer el procedimiento para contrarrestar las posibles fugas de datos para Garantizar la confidencialidad y seguridad de toda la información relacionada con el tráfico de red utilizando políticas DLP del firewall.

2. ALCANCE

Aplica a todos los dispositivos y equipos empleados en las operaciones de Comercializadora rápido S.A. de C.V.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
 Cid Palacios Jesús David Administrador de infraestructura	 Pitol Pimentel Carlos Adrián Gerente de Sistemas	 Martínez Ponce Janely Gestión de Calidad	 Montes Barrera Elliioth Abdel Gerente General

3. REFERENCIAS

ISO 27001:2022 Sistemas de gestión de la seguridad de la información (SGSI)

4. DEFINICIONES Y ABREVIATURAS

4.1 Ataque:

intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

4.2 Amenaza

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

4.3 Confidencialidad:

propiedad de que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados.

4.4 Continuidad de la seguridad de la información:

Procesos y procedimientos para garantizar operaciones continuas de seguridad de la información.

4.5 Incidente de seguridad de la información:


eventos de seguridad de la información únicos o una serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

4.6 Gestión de incidentes de seguridad de la información:

conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de incidentes de seguridad de la información.

Vigente a partir de: 30-ABR-2024	Revisión: 3	Página: 1 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Prevención de Fuga de Datos (DLP)
	Código:	PECRSI17

4.7 DLP:

La función Data Loss Prevention (DLP) o prevención de fuga de datos en los equipos Fortigate permite fijar archivos de carácter sensible para las empresas y en base a eso hacer las detecciones y bloqueos que correspondan para evitar la fuga de dicha información.

4.8 Firewall:

Toda la línea de equipos permite definir individualmente cada una de las interfaces y así darle la posibilidad al equipo a configurar las WAN o DMZ que sean necesarias usando todos los puertos disponibles. Esto permite armar zonas independientes y trabajar sobre ese tráfico que pasa a través de dichas interfaces pudiendo hacer un escaneo de Virus, filtro de URL/IP o simplemente monitorear el tráfico y loguearlo.

4.9 Seguridad de información:

preservación de la confidencialidad, integridad y disponibilidad de la información

Nota 1 a la entrada: Además, también pueden estar involucradas otras propiedades, como autenticidad, responsabilidad, no repudio y confiabilidad.

4.10 Riesgo

Efecto de la incertidumbre sobre los objetivos.

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, positiva o negativa.

Nota 2 a la entrada: La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de, un evento, su consecuencia o probabilidad.

Nota 3 a la entrada: El riesgo a menudo se caracteriza por referencia a “eventos” potenciales, y “consecuencias”, o una combinación de estos.

Nota 4 a la entrada: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la “probabilidad” asociada de que ocurra.

Nota 5 a la entrada: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información.

Nota 6 a la entrada: El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización.

4.11 Criterios de riesgo

Términos de referencia con respecto a los cuales se evalúa la importancia del riesgo.

Nota 1 a la entrada: Los criterios de riesgo se basan en los objetivos organizacionales y el contexto externo y el contexto interno.

Nota 2 a la entrada: Los criterios de riesgo pueden derivarse de normas, leyes, políticas y otros requisitos.

4.12 Vulnerabilidad

Debilidad de un activo o control que puede ser explotado por una o más amenazas.


5. RESPONSABILIDADES

5.1 Gerente General

Aprobar la información documentada del SGC, asegurando que los recursos necesarios estén disponibles para lograr sin problema la implementación efectiva del documento.

Vigente a partir de: 30-ABR-2024	Revisión: 3	Página: 2 de 6
--	-----------------------	--------------------------

“Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada”

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Prevención de Fuga de Datos (DLP)
	Código:	PECRS117

5.2 Gerente de Sistemas IT

Es responsable de garantizar el cumplimiento de este procedimiento para prevenir fuga de datos.

5.3 Administrador de Infraestructura

Es el responsable de la ejecución de las tareas y permisos del fortinet para los equipos, la revisión y verificación de las políticas es actividad esencial y periódica del administrador de infraestructura.

5.4 Auxiliar de Sistemas

Responsable de conocer, atender y asegurar el cumplimiento de las políticas DLP.

5.5 Gestión de Calidad

Gestionar el cumplimiento documental según lo establecido en el SGC, asegura su adecuada implementación, manteniendo la eficacia, así como la mejora continua de estas, resguardando y emitiendo la documentación controlada.

6. DESARROLLO

Se establecen las siguientes políticas con el fin de prevenir la Fuga de Datos:

Políticas para web: este tipo de políticas se encargan de monitorizar el tráfico en la web para determinar la información que viaja por esos protocolos: HTTP DNS

Políticas para correos electrónicos: Este tipo de políticas trabajan sobre los protocolos POP3, SMTP e IMAP para analizar qué tipo de información cruza por dichos protocolos.

Políticas de almacenamiento encriptado: Este tipo de políticas trabajan sobre los datos encriptados que son transferidos FTP NTP MAPI

6.1 DLP en Fortinet

La característica de Prevención de Fuga de Datos o DLP (Data Loss Prevention) permite filtrar los datos que pasan a través de la unidad FortiGate, para evitar que la información considerada sensible o confidencial, que sale fuera de Comercializadora Rápido S.A de C.V. sea vulnerada. Esto se hace a través de la definición de patrones de datos sensibles, de forma que aquellos que pasen a través de FortiGate, serán detectados y bloqueados, o permitidos y registrados (logged).

El perfil de seguridad de DLP se configura desde Políticas → IPv4 → Grupo de direcciones que se le asignará o dirección → Apdo DLP Data Loss Prevention → Selección de sensor → 724DLP.


6.2 Metodología de creación de políticas DLP en Fortinet

Para el desarrollo de políticas DLC se selecciona lo siguiente:

Create new → Activar censor → Editar sensor DLP → Nuevo Filtro → Marca de protocolos → Fin.

Vigente a partir de: 30-ABR-2024	Revisión: 3	Página: 3 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Prevención de Fuga de Datos (DLP)
	Código:	PECRSI17

Ejemplo: DLP en Fortinet

Editar Sensor DLP

Nombre:

default

Comentario:

Log a summary of email and web traffic.

39/255

+

 Crear Nuevo

✎

 Editar Sensor DLP

🗑

 Borrar

Seq #	Tipo	Acción	Servicios	Archivo
No se encontraron entradas coincidentes				

Aplicar

Ejemplo: DLP en Fortinet

FortiGate - FGT_724Navegacion

FortiGate - FG200D_CONEXI...

dlp politicas fortigate - Google...

FortiGate 200D

Sistema

Router

Policy & Objects

Política

IPv4

DoS

Local In

Opciones Proxy

Inspección SSL/SSH

Objetos

Monitor

Acción

ACEPT

opciones Firewall / Network

Habilitar NAT

Use Outgoing Interface

Uso de IP Pool Dinámico

Security Profiles

AntiVirus

Filtro Web

Control de Aplicaciones

IPS

Filtro de Correo

Sensor DLP

Opciones de Proxy

Inspección SSL/SSH

Control de Tráfico

Traffic Shaper Compar

Traffic Shaper Compar

Invertida

Traffic Shaper Por IP

Opciones de Logging

Registrar Tráfico Perm

eventos de seguridad

Todas las sesiones

Capturar paquetes

Comentarios

0/1023

Habilitar esta política

Nueva Política

Editar Sensor DLP

Nuevo Filtro DLP Sensor

Filtro

Mensajes

Archivos

Conteniendo

Tarjeta de Crédito

Expresión Regular

Examine los siguientes servicios

Web Access

HTTP-POST

Email

SMTP

POP3

IMAP

MAPI

Otros

NNTP

Acción

Sólo Log

Archivo

Habilitar

OK

Cancelar


Aplicar

6.3 Habilitar un DLP sensor por política

Seleccione Data Loss Prevention (DLP) → Seleccione la pestaña política → Aparece una lista de las políticas configuradas que admiten DLP. La columna Sensor muestra el sensor habilitado para cada política → Para cambiar el sensor para una o más políticas, seleccione las políticas de la lista → En la lista desplegable

Vigente a partir de: 30-ABR-2024	Revisión: 3	Página: 4 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Prevención de Fuga de Datos (DLP)
	Código:	PECRSI17

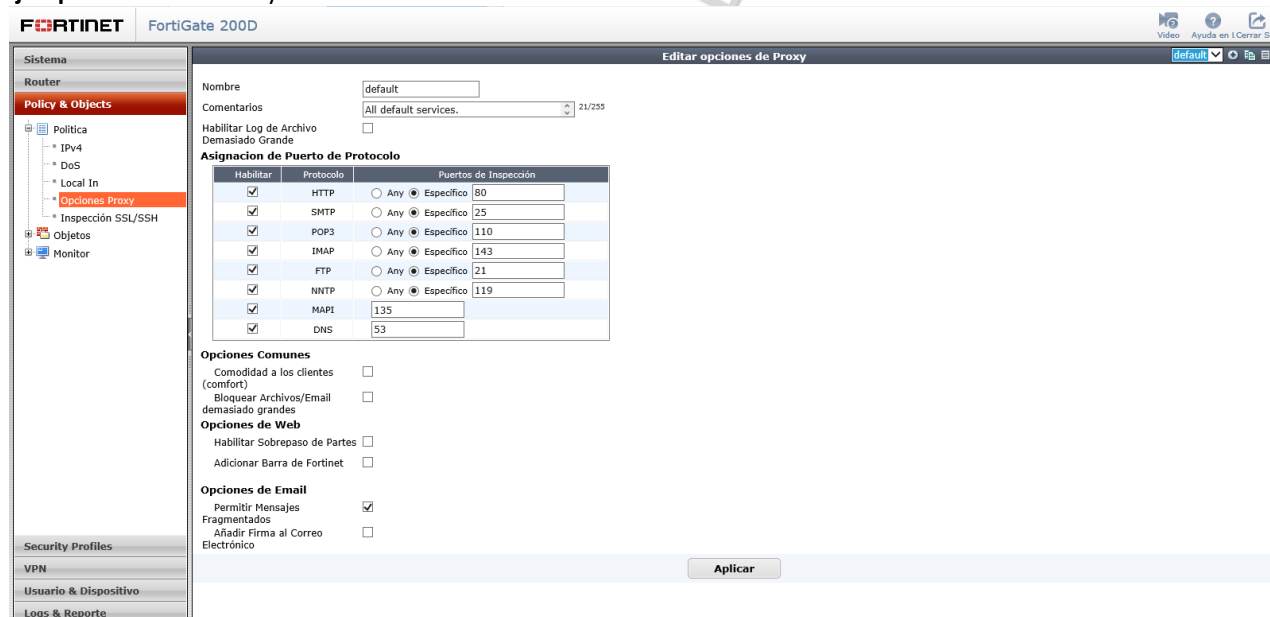
Seleccionar sensor, seleccione el DLP Sensor que se habilitará para las políticas seleccionadas → O bien, para deshabilitar DLP para las políticas seleccionadas, elija Ninguna → Guardar la configuración.

6.4 Seleccionar el DLP sensor en una Acción de Proxy

Para editar los controles de proxy:

Se seleccionan las casillas de habilitación para protocolo → asignando el número de puerto de salida → una vez realizada la acción de proxy se debe seleccionar casilla de las opciones de aplicaciones e-mail → finalizando en la pestaña → Aplicar

Ejemplo: Acción de Proxy



The screenshot shows the FortiGate 200D web interface. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main area is titled 'Editar opciones de Proxy'. The configuration includes:

- Nombre:** default
- Comentarios:** All default services. 21/235
- Habilitar Log de Archivo Demasiado Grande:** ☐
- Asignación de Puerto de Protocolo:**


Habilitar	Protocolo	Puertos de Inspección
<input checked="" type="checkbox"/>	HTTP	<input type="radio"/> Any <input checked="" type="radio"/> Especifico 80
<input checked="" type="checkbox"/>	SMTP	<input type="radio"/> Any <input checked="" type="radio"/> Especifico 25
<input checked="" type="checkbox"/>	POP3	<input type="radio"/> Any <input checked="" type="radio"/> Especifico 110
<input checked="" type="checkbox"/>	IMAP	<input type="radio"/> Any <input checked="" type="radio"/> Especifico 143
<input checked="" type="checkbox"/>	FTP	<input type="radio"/> Any <input checked="" type="radio"/> Especifico 21
<input checked="" type="checkbox"/>	NNTP	<input type="radio"/> Any <input checked="" type="radio"/> Especifico 119
<input checked="" type="checkbox"/>	MAPI	135
<input checked="" type="checkbox"/>	DNS	53
- Opciones Comunes:**
 - Comodidad a los clientes (comfort): ☐
 - Bloquear Archivos/Email demasiado grandes: ☐
- Opciones de Web:**
 - Habilitar Sobrepaso de Partes: ☐
 - Adicionar Barra de Fortinet: ☐
- Opciones de Email:**
 - Permitir Mensajes Fragmentados: ☒
 - Añadir Firma al Correo Electrónico: ☐

At the bottom right, there is an 'Aplicar' button.

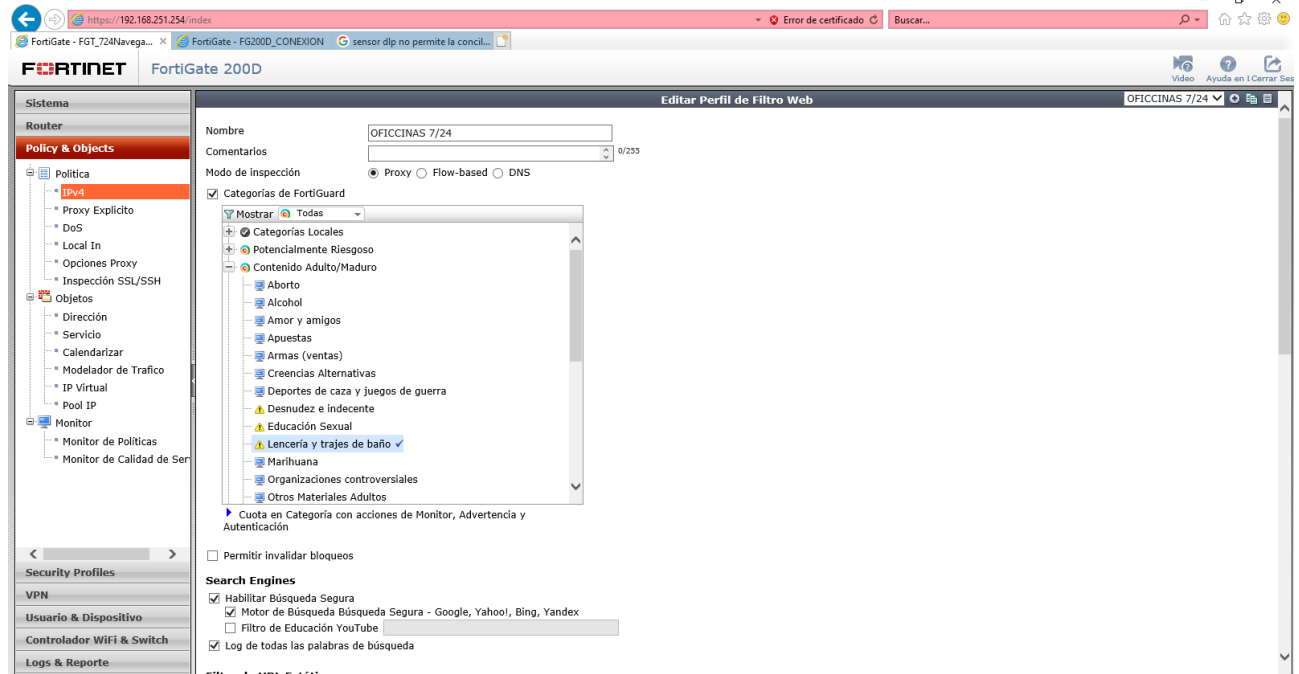
Se puede especificar que ciertos sitios web no sean inspeccionados añadiéndolos a la lista de Modo Inspección, dentro del perfil de inspección correspondiente. Por defecto, la unidad FortiGate tiene como exentas las categorías locales: Potencialmente riesgoso y contenido adulto

Vigente a partir de: 30-ABR-2024	Revisión: 3	Página: 5 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Prevención de Fuga de Datos (DLP)
	Código:	PECRSI17

Ejemplo: Acción de Proxy



7. DIAGRAMA DE FLUJO

Puesto involucrado	Puesto involucrado	Puesto involucrado	Puesto involucrado
NA	NA	NA	NA

8. ANEXOS

TIPO	CODIGO	TITULO
Formato	NA	NA
Ayuda visual	NA	NA
Políticas	NA	NA
Otros (documento externo)	NA	NA

Vigente a partir de: 30-ABR-2024	Revisión: 3	Página: 6 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"