POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

1. Introducción

El plan de gestión de incidentes de seguridad de la información nos permite responder inmediatamente ante un fallo en el sistema, a través de los procedimientos estipulados para realizar la acción correctiva.

2. Objetivo

Determinar los procedimientos para responder ante una falla en el sistema.

3. Alcance

El plan de respuesta a incidentes debe ser utilizado para cada uno de los sistemas dentro del entorno de controles volumétricos.

4. Responsabilidades

Se deben especificar cada uno de los responsables y las actividades que estarán desempeñando durante el proceso.

Actividades	Responsable
Documentar incidentes	Sysadmin
Supervisar, dar seguimiento, notificar los incidentes presentados	Coordinador de tecnologias
Informa y gestiona los incidentes	Gerente de Proyecto
Aprobar documento	Director General

5. Definicion

Incidente de seguridad de la empresa

Un incidente de seguridad de la empresa se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada por la empresa, un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la empresa.

6. Contenido

Funciones y responsabilidades de respuesta a incidentes

Sysadmin

- Documentación específica del incidente.
- Determinar las actividades y acciones requeridas para realizar el escalamiento.
- Notificar y dar respuesta sobre el incidente.
- Brindar las acciones correctivas para remediar el incidente.
- Acciones para lograr el cumplimiento en el entorno de "Controles Volumétricos".
- Descubrimiento de los incidentes.
- Dar informes y respuestas de los incidentes.
- El responsable de monitorear los sistemas debe contar con una disponibilidad de 24 x 7.
- Se debe capacitar al personal sobre las responsabilidades que tiene, cuando se presente una falla de seguridad.

Coordinador Web

- Supervisar los incidentes presentados dentro del entorno de "Controles Volumétricos".
- Debe estar disponible 24x7 para recibir alertas de incidentes.

Comité de seguridad

- Informa y gestiona a la alta dirección los incidentes presentados dentro del entorno de "Controles Volumétricos".
- Audita todos los incidentes presentados y retroalimenta al departamento afectado para mitigar la exposición futura de los datos del contribuyentes.
- Evalúa las políticas y / o procedimientos afectados para determinar si es necesario revisarlos y modificarlos para evitar incidentes similares en el futuro.
- Se deben tener los acuerdos de entendimiento de la seguridad de la información para todas las áreas, incluyendo el área de TIC.

Se deberá de realizar lo especificado en el ***PRT-011-SGSI PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*** como protocolo para la identificación, evaluación, clasificación, registro, atención y seguimiento de incidentes.

Cobertura y respuesta de todos los componentes críticos del sistema

- Se debe tener contemplada la cobertura de todos los componentes críticos del sistema, mediante el documento ***PRT-009-SGSI PROCEDIMIENTO ELABORACIÓN DE MATRIZ DE EVALUACIÓN DE RIESGOS*** contemplando la identificación de los activos críticos y la mitigación de las amenazas y riesgos.

Penalizaciones

La ***POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*** pretende instituir y afianzar la cultura de seguridad de la información entre los empleados, proveedores y partes interesadas de la empresa. Por tal razón, es necesario que las violaciones a las políticas sean clasificadas, con el objetivo de aplicar medidas correctivas, conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información empresarial.

Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo a las circunstancias, si así lo ameritan, estas penalizaciones están señaladas y especificadas en las ***Políticas de la Empresa***.

Directrices para proveedores

Para garantizar la protección de los activos de la organización, que sean accesibles por los proveedores se debe tener en cuenta lo siguiente:

- Se debe elaborar y aprobar la Cláusula, convenios de prestación de servicio y/o Acuerdos de confidencialidad, en los cuales se debe especificar: Los servicios, informes y registros suministrados por terceros son monitoreados y revisados regularmente, y las auditorías se realizan a intervalos regulares.
- Ante alguna falta a la relación por parte del proveedor, podría provocar la cancelación del servicio.

En el caso de presentarse incidentes de seguridad por parte del proveedor de infraestructura on premise o servicios en la nube, el proveedor asignado deberá completar el siguiente protocolo de notificación para el cliente en este caso Pegasus.

1-. Al tener el conocimiento concreto respecto al incidente de seguridad generado, el proveedor deberá realizar una notificación de forma inmediata, de manera verbal y escrita (vía correo electrónico) al responsable de esa área dentro del equipo del cliente, esta notificación se generará de acuerdo al documento **DOC-018-SGSI MATRIZ DE ESCALAMIENTO DE CONTACTO EN CASO DE INCIDENTE.**

2-. El receptor al tener la notificación del incidente deberá generar una notificación de recibido la cual se deberá enviar al respectivo proveedor.

3-. Una vez enviada la notificación el receptor deberá seguir los lineamientos establecidos en la política **POL-008-SGSI POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** en el cual se establecen las acciones a realizar para proteger la seguridad de la información.

4-. En caso de que el proveedor no reciba la notificación por parte del receptor deberá reintentar toda la matriz hasta recibir la confirmación correspondiente.

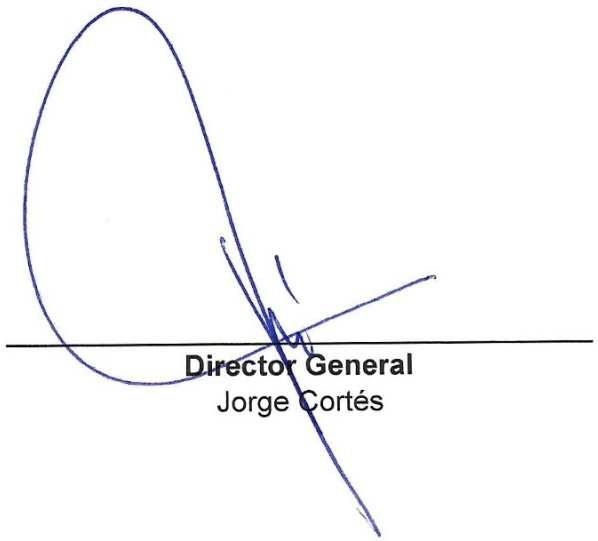
Observaciones

DOC-030-SGC REPORTE DE INCIDENTES CONTROLES VOLUMÉTRICOS en el cual se identifica el seguimiento y cierre de incidentes y la notificación a los puestos directivos.

7. Historial de Revisiones

Versión	Fecha	Cambios	Elaboró	Revisó	Aprobó
1.0	11/06/2019	Creación de documento	Carmen Nuñez	Rubén Villafuerte	Rubén Villafuerte
1.1	11/03/2020	Actualización tiempo de cambios cada tres meses	Carmen Nuñez	Rubén Villafuerte	Rubén Villafuerte
1.2	08/06/2020	-Cambio de nomenclatura -Corrección de contenido	Elvira Partida	Rubén Villafuerte	Rubén Villafuerte
1.3	29/01/2021	Actualización de responsabilidades	Elvira Partida	Rubén Villafuerte	Rubén Villafuerte
1.4	12/10/2021	Actualización de firmas compromiso	Omar Aguilar	Rubén Villafuerte	Rubén Villafuerte
1.5	06/12/2022	Revisión de documento	Omar Aguilar	Rubén Villafuerte	Rubén Villafuerte

8. Firmas compromiso



Director General
Jorge Cortés

Gerente de Proyecto
Ruben Villafuerte

Coordinador de Tecnologías
Fabián Candelario

Sysadmin
Fabián Candelario