PD.GA.27

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

EMCANDELARIA
Empresas Municipales de Candelaria

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Tener un sistema organizado y bien planificado que permita gestionar adecuadamente los incidentes de seguridad de la información que se presenten en EMCANDELARIA S.A.S. E.S.P, definiendo acciones para identificar, analizar, clasificar, valorar y dar respuestas pertinentes en busca de la solución de los incidentes que ocurran a con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

La gestión de incidentes de seguridad empieza desde el reporte hasta el cierre y finalización del incidente, comprende las siguientes fases:

- ✔ Reporte y registro en formato orden de servicio del evento y/o incidente de seguridad de la información.
- ✔ Evaluación inicial del reporte.
- ✔ Análisis y evaluación del impacto.
- ✔ Aplicación de acciones de contención y acciones complementarias.
- ✔ Documentación de lecciones aprendidas.
- ✔ Notificación de cierre del evento y/o incidente.

Este procedimiento requiere del cumplimiento por parte de funcionarios, contratistas y terceros.

3. RESPONSABLES

Profesional de Gestión Informática y Comunicaciones: encargado de gestionar los servicios de TI.
Gestor de Mesa de Ayuda: responsable de administrar la aplicación de la mesa de ayuda.
Equipo Técnico de Soporte: responsable de dar el soporte a los incidentes reportados en el primer nivel según lo escale la mesa de ayuda.
Profesional de Seguridad de la Información: responsable de dar respuesta a los incidentes de Seguridad de la Información según lo escale la mesa de ayuda.

4. DEFINICIÓN DE TÉRMINOS

Activo de Información: En el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y, por lo tanto, debe proteger”. Se puede considerar como un activo de información a: Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.

Amenaza: se refiere a cualquier cosa que tenga el potencial de causar daño grave a un sistema o activo de información, una amenaza es algo que puede suceder o no, pero tiene el potencial de causar daño grave.

Analista de Mesa de Servicio: Recibe la información de los Colaboradores de EMCANDELARIA S.A.S E.S.P, toma el formato de orden de servicio diligenciado y es el primer contacto para la gestión de los incidentes de seguridad.

Ataque informático: Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.

Ciberataque: es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que ataquen a sistemas de información, como lo son infraestructuras, redes computacionales, o bases de datos que están albergadas en servidores remotos. Estas maniobras son realizadas por medio de actos maliciosos usualmente originados de fuentes anónimas y direcciones que no pueden ser rastreadas.

Código malicioso: Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

COLCERT: Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Contención de un incidente: Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.

CSIRT: Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.

Denegación del servicio: Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema o servicio informático.

Equipo de Respuesta a incidentes: Equipo conformado por Colaboradores y/o terceros asociados (operadores estratégicos) que cuentan con las habilidades y competencias para tratar los incidentes de seguridad durante el ciclo de vida de éstos.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2009].

Evento de seguridad de la información: Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].

Incidente de seguridad de la información: Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción de información no autorizada; además de un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información que atente contra la misionalidad de la entidad.

Incidente de continuidad tecnológica: Evento intencionado o no intencionado que puede afectar los servicios que presta el proceso de Tecnología de la información y de las comunicaciones.

Malware: software malicioso que tiene como objetivo infiltrarse en algún sistema de información sin autorización y de esta forma dañar o perjudicar al propietario de la misma

Phishing: Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso del banco.

Plan de continuidad de la operación: (BCP. Business Continuity Plan): Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

Ransomware: Piezas de código desarrolladas por atacantes informáticos para secuestrar información de los equipos infectados a través de técnicas

criptográficas y posteriormente solicitar el pago de rescate para la recuperación de información.

Seguridad Digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de Ciberdefensa que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Suplantación de identidad: Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

5. POLITICA DE OPERACIÓN

Los posibles incidentes de seguridad y/o eventos se reportarán a la Mesa de ayuda a través de los siguientes canales:

- ✔ Enviando un mensaje de correo electrónico con el formato de orden de servicio al correo electrónico james.wilches@emcandelaria.gov.co y cristian.bravo@emcandelaria.gov.co.

- ✔ Llamando a los números de contacto celular de el responsable de la mesa de ayuda o el Profesional de Seguridad de la Información designado.

El funcionario que identifique el posible ataque y/o evento de seguridad debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención de este, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.

Una vez se reciba el formato de calidad de orden de servicio debidamente diligenciado del posible Incidente o del evento de seguridad, el analista de la mesa de ayuda debe realizar y analizar la categorización, para iniciar con la atención del mismo, si cumple con algunos de los siguientes criterios puede ser considerado como un incidente de seguridad, de lo contrario se tratará como un evento falso positivo o como un incidente de tecnología.

- Hubo daño o pérdida de información física o digital.
- Hubo fuga y/o robo de información física o digital.
- Hubo robo de credenciales o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, Ransomware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.
- Uso indebido de imagen institucional.
- Se presentó la suspensión de algún servicio de tecnología.
- Se presentó caída y suspensión de la página Web Institucional.

DESCRIPCION DEL PROCEDIMIENTO

ACTIVIDAD	RESPONSABLE	REGISTRO
REGISTRO DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN El usuario (propietario y/o funcionario de la información) reporta el incidente de seguridad que identifique o reconozca a la mesa de ayuda de acuerdo al PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DE EMCANDELARIA S.A.S E.S.P.	Usuario (propietario y/o funcionario de la información)	Diligenciamiento formato de calidad Orden de Servicio

IDENTIFICACION Y CATEGORIZACIÓN DEL INCIDENTE El gestor de la mesa de ayuda se encarga de analizar e identificar el incidente con el fin de priorizar, categorizar como seguridad de la información y asignarlo al Profesional o líder de Seguridad de la Información encargado.	Gestor de Mesa de Ayuda	Formato de calidad Orden de Servicio
INFORMAR AL USUARIO Se informa al propietario y/o funcionario de la información asociado al incidente para que no sea manipulado el activo de información relacionado por él o por más personas de su área.	Profesional o líder de Seguridad de la Información	Correo electrónico institucional
ANÁLISIS DEL INCIDENTE DE SEGURIDAD Ejecutar las actividades de análisis pertinentes en busca de la solución del incidente de seguridad. En caso que el análisis determine que requiere contacto con las autoridades externas oficiales se debe notificar.	Profesional o líder de Seguridad de la Información	Notificar autoridades externas
CONTACTO CON LAS AUTORIDADES Contactar a las entidades externas oficiales que dan soporte a incidentes de seguridad de la información tales como COLCERT, CSIRT de Gobierno, Fiscalía y DIJIN de acuerdo al procedimiento.	Profesional o líder de Seguridad de la Información	Correo electrónico institucional
RECOLECCIÓN DE EVIDENCIAS Se identifica, recolecta y documenta todas las evidencias asociadas al incidente de seguridad según el procedimiento: Identificación, Recolección, Adquisición y Preservación de Evidencias	Profesional o líder de Seguridad de la Información	Evidencia física o digital identificada y recolectada
TRATAMIENTO DEL INCIDENTE El profesional de seguridad de la información en conjunto con el área de informática, desarrollaran las actividades necesarias para dar tratamiento al incidente de seguridad, documentando en la mesa de ayuda las actividades realizadas.	Profesional o líder de Seguridad de la Información	Registro en bitácora mesa de ayuda
APRENDIZAJE ASOCIADO AL INCIDENTE Se documenta todo el conocimiento adquirido asociado a la identificación, análisis y respuesta del incidente de seguridad con el fin de reducir la posibilidad y el impacto en futuros incidentes.	Profesional o líder de Seguridad de la Información	Registro en bitácora mesa de ayuda

CERRAR INCIDENTE Si el incidente se solucionó finaliza el procedimiento y se procede a cerrarlo de acuerdo al procedimiento. Si el incidente no se solucionó se devuelve a la actividad **ANÁLISIS DEL INCIDENTE DE SEGURIDAD**	Profesional o líder de Seguridad de la Información	Registro en bitácora mesa de ayuda

Control de Cambios

Fecha	Versión	Cambios
17/08/2022	1	Adopción procedimiento

Elaboró	Revisó	Aprobó
Líder Seguridad de la información Ing. Cristian Felipe Bravo	Líder Control interno Mithchelle Leonel Martínez	