POLÍTICA INTERNA DE CIBERSEGURIDAD DE LA CORPORACIÓN CAMBIO SOSTENIBLE

1. INTRODUCCIÓN

La presente Política Interna de Ciberseguridad establece las pautas y directrices para prevenir, detectar y responder a amenazas cibernéticas, con un enfoque especial en la mitigación de ataques de *ransomware*. Cambio Sostenible, reconoce la importancia crítica de salvaguardar la integridad, confidencialidad y disponibilidad de su información, especialmente tras la experiencia de un ciberataque en 2023 que evidenció la urgente necesidad de fortalecer las medidas de seguridad digital. Esta política adopta las recomendaciones aplicables a la Guía de Seguridad Digital de Conexo en su versión más reciente como parámetro de la seguridad digital y privacidad de la organización.

1.1 Contexto Organizacional

Cambio Sostenible, como entidad sin ánimo de lucro, enfrenta constantes desafíos en el entorno digital, incluyendo ciber-amenazas. La organización gestiona información sensible relacionada con derechos humanos, medio ambiente y otros temas cruciales. El contexto organizacional destaca la necesidad de medidas de ciberseguridad efectivas para preservar la integridad de los datos y la continuidad de las operaciones.

1.2 Justificación

La creciente sofisticación de las amenazas cibernéticas, especialmente los ataques de *ransomware*, resalta la necesidad crítica de una política interna de ciberseguridad. La justificación de esta política radica en la protección proactiva de la información y los sistemas de la organización, basándose en la lección aprendida tras el ciberataque sufrido en 2023, que subrayó la importancia de una respuesta y defensa efectivas ante amenazas digitales.

1.3 Alcance y Objetivos

1.3.1 Alcance

Esta política abarca todas las operaciones y procesos digitales de Cambio Sostenible, incluyendo, pero no limitándose a, la gestión de correos electrónicos, almacenamiento en la nube, comunicaciones internas y externas, y el manejo de datos de los miembros y colaboradores.

1.3.2 Objetivos

- Preservar la confidencialidad, integridad y disponibilidad de la información.
- Mitigar el riesgo de ataques de ransomware y otras amenazas cibernéticas.
- Establecer prácticas de seguridad digital para todos los colaboradores.
- Garantizar la continuidad de las operaciones frente a incidentes de seguridad.

2. DEFINICIONES CLAVE

2.1 *Ransomware*

El *ransomware* es un tipo de software malicioso diseñado para bloquear el acceso a un sistema o archivos, generalmente mediante cifrado, con el propósito de extorsionar a la víctima para que

realice un pago a cambio de restablecer el acceso. Este término incluye variantes como el cifrado de archivos y el secuestro de sistemas, representando una seria amenaza para la confidencialidad e integridad de los datos.

2.2 Activos de Información

Los activos de información comprenden cualquier recurso o dato valioso para Cambio Sostenible, incluyendo, pero no limitándose a, información de proyectos, datos de miembros, comunicaciones internas y externas, documentos legales, contratos y cualquier otro contenido digital de relevancia para la organización.

2.3 Amenazas Cibernéticas

Las amenazas cibernéticas son acciones o eventos maliciosos que buscan comprometer la seguridad de los sistemas informáticos y la información digital. Incluyen, entre otras, virus, malware, phishing, ataques de fuerza bruta y, específicamente, ataques de ransomware. Estas amenazas representan riesgos potenciales para la integridad y confidencialidad de los activos de información.

3. RESPONSABILIDADES Y ROLES

3.1 Dirección Ejecutiva

La Dirección de Cambio Sostenible tiene la responsabilidad general de garantizar la implementación y el cumplimiento de la política de ciberseguridad. Esto incluye la asignación de recursos adecuados y la toma de decisiones estratégicas para mitigar los riesgos asociados con ciberamenazas, especialmente el *ransomware.*

3.2 Responsable de Ciberseguridad

Se designará a un miembro del equipo como el Responsable de Ciberseguridad, quien será el encargado de supervisar la aplicación de esta política y coordinar las actividades relacionadas con la seguridad cibernética. Este rol incluirá la actualización continua de las medidas de seguridad, la respuesta a incidentes y la comunicación interna sobre las amenazas emergentes.

3.3 Usuarios y Colaboradores

Todos los usuarios y colaboradores de Cambio Sostenible tienen la responsabilidad de conocer y cumplir con las prácticas de seguridad establecidas. Esto implica seguir las directrices proporcionadas, informar cualquier incidente de seguridad de inmediato y participar en sesiones de capacitación periódicas para mantenerse informado sobre las mejores prácticas de ciberseguridad.

3.4 Asamblea General y Junta Directiva

La Asamblea General y la Junta Directiva revisarán y aprobarán esta política, asegurándose de que esté alineada con los objetivos estratégicos de la organización. Además, serán responsables de asignar los recursos necesarios para implementar medidas de seguridad efectivas contra *ransomware* y otras amenazas cibernéticas.

3.5 Proveedor de Servicios de TI

En caso de que Cambio Sostenible utilice servicios de terceros para la gestión de TI: proveedores de nube, alojamiento, dominio, correos, sistemas de información y asociados, el proveedor de servicios tendrá la responsabilidad de implementar medidas de seguridad adecuadas para proteger los sistemas y datos de la organización contra amenazas, incluyendo ransomware. Esto debe ser revisado por el/la responsable de la ejecución de esta política previo a la contratación de los servicios, este deberá emitir a la dirección concepto oral o escrito favorable o no sobre la garantía de protección que ofrece el proveedor en sus cláusulas contractuales.

4. MEDIDAS DE PREVENCIÓN Y PROTECCIÓN

4.1 Actualizaciones y Parches

Es fundamental mantener todos los sistemas y software actualizados con las últimas versiones y parches de seguridad. La Responsabilidad de Ciberseguridad supervisará regularmente la disponibilidad de actualizaciones y garantizará su implementación oportuna.

4.2 Antivirus y Antimalware

Todos los dispositivos conectados a la red de Cambio Sostenible deben tener instalado software antivirus y antimalware actualizado. Se realizarán escaneos periódicos para detectar y eliminar posibles amenazas.

4.3 Concientización y Capacitación

Se llevarán a cabo encuentros internos regulares de concientización y capacitación para todos los usuarios y colaboradores. Estos programas abordarán las mejores prácticas de seguridad, la identificación de posibles amenazas y la respuesta adecuada ante incidentes de ciberseguridad.

4.4 Copias de Seguridad Regulares

Se realizarán copias de seguridad regulares de todos los datos de los sistemas *online* con una frecuencia semestral. Estas copias se almacenarán en ubicaciones seguras y se probarán periódicamente para garantizar su integridad y restauración efectiva en caso de un ataque de *ransomware* u otro incidente. Además, Cambio Sostenible contará con un disco (*hardware*) para almacenamiento de información fuera de línea, este deberá ser actualizado en copias de seguridad con una frecuencia mínima de 4 meses, la responsabilidad de esta descarga de información será de la Dirección, y deberá notificarse a la persona responsable de la ejecución de esta política vía correo electrónico que incluya la fecha y detalles del resguardo de información.

4.5 Restricciones de Acceso y Privilegios

Se implementarán restricciones de acceso basadas en roles y privilegios para limitar el acceso a sistemas y datos, esto en virtud de dar cumplimiento a los roles asignados en la Política de Tratamiento de Datos de la organización. Sólo se otorgarán privilegios necesarios para realizar tareas específicas, reduciendo así el riesgo de acceso no autorizado.

4.6 Firewall y Filtros de Contenido

Se configurarán y mantendrán firewalls en todos los dispositivos y en la red para monitorear y filtrar el tráfico. Además, se aplicarán filtros de contenido para prevenir la descarga o acceso a contenido

malicioso.

PARÁGRAFO ÚNICO:

Previo encuentro articulado con el Registro de Direcciones de Internet de América Latina y Caribe (LACNIC) a través del Programa FRIDA, se acuerda que Cambio Sostenible utilizará el mecanismo de reporte del CSIRT (*Computer Security Incident Response Team*, Equipo de Respuesta ante Incidencias de Seguridad Informáticas) quien tiene como misión: Llevar a cabo las funciones de coordinación necesarias para el fortalecimiento de las capacidades de respuesta a incidentes vinculados a los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa de América Latina y el Caribe, en el marco de las metas específicas establecidas por la misión de LACNIC tendientes a lograr el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento.
El enlace para reporte de incidentes asociados a DOS, DDOS, *email abuse*, fuerza bruta, *intrusion attempt, malware, pharming, pishing, redirect, PAC, proxy, unauthorized prefix advertising* y otros, será: https://csirt.lacnic.net/reportar-incidente

5. RESPUESTA ANTE INCIDENTES

5.1 Procedimientos de Respuesta

Esta ruta permitirá responder como organización social ante incidentes de ciberseguridad. Esto incluirá la notificación inmediata a la Responsabilidad de Ciberseguridad y la implementación de medidas para contener y mitigar el incidente.

5.2 Equipo de Respuesta

La persona responsable de la implementación de esta política, designará un Equipo de Respuesta ante Incidentes (IRT) compuesto por personal con habilidades especializadas en ciberseguridad. Este equipo liderará la respuesta, la recuperación y la comunicación interna y externa durante un incidente.

5.3 Comunicación durante Incidentes

Se establecerá un protocolo de comunicación para informar a los interesados internos y externos sobre cualquier incidente de ciberseguridad. La comunicación será transparente, oportuna y coordinada por el Equipo de Respuesta ante Incidentes.

5.4 Evaluación Posterior al Incidente

Después de cualquier incidente de ciberseguridad, se realizará una evaluación exhaustiva para identificar lecciones aprendidas y áreas de mejora. Esta evaluación ayudará a fortalecer las medidas de seguridad y prevenir incidentes similares en el futuro.

5.5 Colaboración con Autoridades Competentes

En caso de incidentes graves, se colaborará plenamente con las autoridades competentes en Colombia, incluyendo informes detallados y la implementación de acciones recomendadas. Desde Cambio Sostenible y en cumplimiento con su función social de organización que se dedica a realizar acciones meritorias, se promueve el uso de la denuncia ante los entes garantes de derechos como

la Delegada para Ambientes Digitales de la Defensoría del Pueblo e impulsores de causas penales asociadas a la criminalidad en internet como la Fiscalía General de la Nación en cumplimiento de la ley 1273 de 2009.

5.6 Fondo Especial para Reparación de Daños y Restitución de Sistemas

Ante la ocurrencia de un incidente de ciberseguridad, se establecerá un Fondo Especial para Reparación de Daños y Restitución de Sistemas. Este fondo se utilizará exclusivamente para cubrir los costos asociados con la reparación y restitución de sistemas afectados por el incidente. El Equipo de Respuesta ante Incidentes (IRT) será responsable de manejar este fondo y elegir los mecanismos que garanticen una rápida y efectiva recuperación de los sistemas comprometidos.

La tesorera, como miembro de la Junta Directiva, será la encargada de gestionar el fondo. Se compromete a ponerlo a disposición del IRT en un plazo máximo de 12 horas posteriores a la ocurrencia del incidente, asegurando así una respuesta ágil y oportuna para minimizar los impactos del incidente en la organización.

5.7 Servicios de Restauración

En caso de que sea necesario, el Equipo de Respuesta ante Incidentes (IRT) estará encargado de cotizar y contratar servicios para la restauración de los sistemas afectados en un plazo máximo de 72 horas posteriores a la ocurrencia del incidente. Estos servicios pueden incluir la restauración de servicios asociados al hosting, dominio o sistemas internos comprometidos.

Esta medida garantiza que Cambio Sostenible pueda recuperar rápidamente sus servicios esenciales en caso de un incidente grave de ciberseguridad. Si la organización no cuenta con la capacidad técnica para realizar la restauración por sí misma, el IRT tomará las medidas necesarias para contratar a proveedores externos especializados, asegurando así una pronta recuperación y minimizando los impactos del incidente en la operatividad de la organización.

6. FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD

6.1 Programas de Formación Continua

Se implementarán programas regulares de formación en ciberseguridad para todo el personal de Cambio Sostenible. Esto incluirá la identificación de amenazas, prácticas seguras de navegación, y la conciencia sobre los riesgos asociados con los correos electrónicos y enlaces sospechosos.

6.2 Simulacros de Phishing

Se llevarán a cabo simulacros periódicos de phishing para evaluar la resistencia del personal ante posibles ataques de ingeniería social. Estos ejercicios proporcionarán oportunidades de aprendizaje y permitirán ajustar las estrategias de formación.

6.3 Sensibilización sobre *Ransomware*

Se organizarán sesiones de sensibilización específicas sobre ransomware, destacando las tácticas utilizadas por los atacantes, los signos de posibles amenazas y las medidas preventivas a tomar.

6.4 Actualización Continua sobre Amenazas

El personal recibirá actualizaciones periódicas sobre nuevas amenazas y tácticas utilizadas por los ciberdelincuentes. Esto garantizará que estén informados sobre las últimas tendencias en ciberseguridad.

6.5 Responsabilidad Individual y Colectiva

Se fomentará la responsabilidad individual y colectiva en materia de ciberseguridad. Cada miembro de Cambio Sostenible tendrá un papel crucial en la protección de los activos de información y la prevención de incidentes.

7. GESTIÓN DE INCIDENTES

7.1 Procedimientos de Respuesta a Incidentes

Se establecerán procedimientos claros y detallados para responder eficientemente a incidentes de seguridad, con un enfoque específico en ataques de ransomware. Esto incluirá la notificación inmediata a las partes relevantes y la activación de un equipo de respuesta.

7.2 Equipo de Respuesta a Incidentes

Se designará y capacitará a un equipo de respuesta a incidentes encargado de coordinar las acciones de mitigación, contención y recuperación. Este equipo actuará de manera rápida y efectiva para minimizar el impacto de los incidentes.

7.3 Evaluación Post-Incidente

Tras la resolución de un incidente, se llevará a cabo una evaluación exhaustiva para identificar las lecciones aprendidas y mejorar continuamente los procedimientos de respuesta.

7.4 Comunicación Externa e Interna

Se establecerán protocolos claros para la comunicación interna y externa durante y después de un incidente. La transparencia y la gestión adecuada de la información serán fundamentales para mantener la confianza de los interesados.

7.5 Respaldo de Datos y Sistemas

Se implementarán políticas de respaldo robustas para garantizar la disponibilidad y recuperación rápida de datos y sistemas afectados durante un ataque de *ransomware.*

7.6 Evaluación de Vulnerabilidades Post-Incidente

Después de un incidente, se llevará a cabo una evaluación de vulnerabilidades para identificar posibles brechas en la seguridad y tomar medidas correctivas.

8. EVALUACIÓN Y REVISIÓN CONTINUA

8.1 Auditorías de Seguridad

Se realizarán auditorías de seguridad periódicas para evaluar la efectividad de las medidas implementadas y garantizar el cumplimiento de la política interna de ciberseguridad.

8.2 Actualización de Políticas y Procedimientos

La política interna de ciberseguridad se revisará y actualizará de manera regular para adaptarse a las cambiantes amenazas y tecnologías. Todas las actualizaciones se comunicarán de manera efectiva a los miembros relevantes de la organización.

8.3 Formación Continua

Se llevarán a cabo sesiones de formación continua para sensibilizar a los empleados sobre las últimas amenazas de seguridad y garantizar que estén equipados para reconocer y responder adecuadamente a posibles ataques.

8.4 Colaboración Externa

La organización buscará colaborar con expertos externos en ciberseguridad para obtener información actualizada y mejores prácticas. La participación en comunidades de seguridad y la asistencia a eventos del sector serán fomentadas.

8.5 Métricas de Seguridad

Se establecerán métricas de seguridad claras para evaluar la efectividad de las medidas de ciberseguridad y garantizar una mejora continua.

9. RESPONSABILIDADES

9.1 Junta Directiva

La Junta Directiva será responsable de la supervisión general de la implementación de la política interna de ciberseguridad y garantizará que se asignen los recursos adecuados.

9.2 Responsable de Ciberseguridad

Se designará a un Responsable de Ciberseguridad dentro de la organización, quien será el encargado de liderar la implementación, supervisión y revisión continua de las medidas de seguridad.

9.3 Personal y Miembros

Todos los empleados y miembros de la organización tienen la responsabilidad de seguir las prácticas y procedimientos de ciberseguridad establecidos, participar en la formación continua y reportar cualquier incidente de seguridad.

9.4 Evaluación y Auditorías

El equipo de evaluación y auditorías se encargará de realizar auditorías periódicas para garantizar el cumplimiento de las políticas de ciberseguridad y propondrá mejoras según sea necesario.

10. REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

10.1 Ciclos de Revisión

La política será sometida a revisiones regulares para garantizar su vigencia y relevancia. Se establecerá un ciclo de revisión semestral para evaluar la efectividad de las medidas de seguridad y realizar las actualizaciones necesarias.

10.2 Actualización Continua

La política será actualizada de manera continua en respuesta a cambios en el entorno de amenazas, nuevas tecnologías y mejores prácticas en ciberseguridad. La actualización será realizada por el responsable designado y comunicada a todos los miembros del personal de manera oportuna.

10.3 Aprobación de la Actualización

Cada actualización será sometida a aprobación por parte del responsable de seguridad de la información antes de su implementación, asegurando así su conformidad con los estándares de seguridad establecidos.

11. APROBACIÓN Y VERSIONAMIENTO

11.1 Responsables de la Aprobación

La aprobación de la política estará a cargo del responsable designado para la seguridad de la información. Se garantizará que este responsable tenga el conocimiento y la autoridad necesarios para respaldar la implementación efectiva de la política.

11.2 Control de Versiones

Se establecerá un sistema de control de versiones para documentar y rastrear los cambios realizados en la política. Cada versión contendrá un historial de modificaciones, fechas de revisión y los responsables de la aprobación. La numeración de versiones seguirá un formato claro y comprensible para facilitar la identificación de la última versión en vigor.

11.3 Comunicación de Cambios

Cualquier cambio realizado en la política será comunicado de manera efectiva a todo el personal relevante. Se utilizarán canales internos de comunicación para garantizar que los miembros de la organización estén informados sobre las actualizaciones y comprendan cómo afectan a sus responsabilidades y prácticas laborales.

12. DESIGNACIONES

La junta directiva aprueba designar a Diana Carolina Prieto Herrera como responsable de la implementación de esta Política Interna de Ciberseguridad quien ha aceptado libremente el nombramiento en fecha 06 de febrero de 2024.

Elaboró: Kenny S. Espinoza Velásquez

Revisó y aprobó: Yiseth Cruz