Oficio Nro. SEPS-SGD-IGT-2021-21112-OFC

Quito, D.M., 23 de agosto de 2021

Asunto: Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario.

SEÑORES GERENTES
ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

De mi consideración:

Bajo la coyuntura actual, en la que la pandemia mundial del COVID-19 ha marcado un punto de inflexión, la dependencia de la infraestructura tecnológica, la transformación digital de las economías, las transacciones y el acceso a plataformas móviles de servicios financieros, han experimentado una aceleración.

De acuerdo con lo anterior, es prácticamente un hecho que los ataques cibernéticos, el cibercrimen y los incidentes de seguridad no van a disminuir; por el contrario, aumentarán de forma exponencial en los próximos años.

En la misma línea, considerando que la Ciberseguridad está entre los cinco riesgos globales más relevantes, surge la necesidad de que las entidades de la Economía Popular y Solidaria, desde su planeación estratégica, incluyan proyectos, políticas y controles de Ciberseguridad.

En ese sentido, la Superintendencia de Economía Popular y Solidaria (SEPS) tal como se determina en la normativa legal vigente en concordancia a la resolución SEPS-IGT-IR-IGJ-2018-0279 referente a la *Norma de Control para la Administración del Riesgo Operativo y Riesgo Legal en las entidades del Sector Financiero Popular y Solidario Bajo el Control de la Superintendencia de Economía Popular y Solidaria* y alineada a los marcos de referencia de Seguridad de la Información/Ciberseguridad, ve la necesidad de presentar algunas ***recomendaciones*** que permitirán a las entidades controladas actuar de manera oportuna y eficiente ante los posibles ataques informáticos que pudieran quebrantar la integridad, confidencialidad y disponibilidad de la información.

Introducción

Se recomienda la implementación de la triada preventiva[1] cuya finalidad es mitigar el riesgo inherente de las entidades y con ello reducir la posibilidad de materializar un incidente.

Oficio Nro. SEPS-SGD-IGT-2021-21112-OFC

Quito, D.M., 23 de agosto de 2021

N°	Recomendación	Acción
1	Inventario de activos de información.	Identificar y cuantificar los activos de información existentes y dónde están ubicados.
2	Clasificación de información.	Clasificar los activos de información para garantizar una eficaz gestión de su seguridad con criterios de confidencialidad, disponibilidad e integridad.
3	Análisis y evaluación de riesgos de las aplicaciones, servicios y activos.	Relacionar los peligros y las vulnerabilidades con el fin de determinar el nivel de riesgo; se puede usar cualquier método de gestión de riesgos de seguridad de la información, con preferencia por métodos o metodologías documentadas, estructuradas y generalmente aceptadas.
4	Identificación de los procesos críticos.	Definir los procesos críticos de la Entidad y el flujo de la información.
5	Respaldos y resguardo de información sensible.	Respaldar información sensible en lugares adecuados, además de **verificar el correcto funcionamiento de los respaldos,** garantizando el óptimo restablecimiento de operaciones en caso de ser necesario.
6	Cultura de seguridad de la información y ciberseguridad dentro de la entidad.	Crear un ambiente de compromiso y aprendizaje continuo de todos los colaboradores tanto internos como externos, ya sea mediante capacitaciones, charlas continuas, entregándoles procedimientos y pasos a ser ejecutados con el fin de mantener segura la información, bajo indicadores para la medición de madurez, y así proponer

		estrategias que permitan mitigar y anticipar cualquier evento de riesgo.
7	Planes de Contingencia, con procesos y procedimientos a ejecutarse.	Elaborar los planes de contingencia, verificarlos periódicamente para que permitan tomar acciones emergentes sobre eventos que afecten la disponibilidad de los servicios de la entidad.
8	Normativa interna de Seguridad de la Información y ciberseguridad.	Elaborar, actualizar y/o adoptar normativa de relacionada con la seguridad de la información y ciberseguridad en la entidad.
9	Credenciales seguras en infraestructura y usuarios finales.	Elaborar e implementar políticas y/o procedimientos específicos de credenciales seguras para infraestructura y usuarios finales.

Controles específicos de Ciberseguridad sugeridos

La utilización del internet y el acceso a la información digital permiten el crecimiento de las entidades incrementado la productividad de éstas, además de la posibilidad de generar procesos eficaces y eficientes creando mejores oportunidades de consumo de información; sin embargo, también pueden conllevar ciertos riesgos, por lo que es necesario tomar acciones para abordar estos riesgos de forma estructurada.

La Ciberseguridad, es un entorno dinámico y cambiante que requiere una vigilancia continua; además de actualizaciones, pruebas, parches y cambios en concordancia con los avances en el aspecto tecnológico y evolución del negocio. La Superintendencia considera que implementar controles es un punto fundamental para mantener la seguridad dentro de la infraestructura tecnológica de las entidades. El no abordar estos procesos de control se convierte en una de las principales causas para la exposición de brechas de seguridad, en este sentido recomendamos la implementación de al menos los siguientes controles sin perjuicio de la aplicación de medidas adicionales y/o complementarias.

Oficio Nro. SEPS-SGD-IGT-2021-21112-OFC

Quito, D.M., 23 de agosto de 2021

N°	Control	Descripción
1	Gestión de identidades.	Las entidades delimitarán los diversos procesos de negocio para el manejo de identidades y credenciales de los empleados desde el ingreso hasta su desvinculación.
2	Aprovisionamiento, des-aprovisionamiento, bloqueo y desbloqueo de cuentas de usuario.	Las entidades deberán crear cuentas de usuario, las mismas que estarán activas hasta el momento en que el usuario se desvincule de la entidad.
3	Gestión y Autorización de Usuarios.	Las entidades utilizarán procesos de gestión y autorización, usando controles de acceso para identificar y diferenciar usuarios según sus funciones considerando las siguientes características: • Limitar el acceso privilegiado a solo aquellos que lo requieran. • Realizar verificaciones de antecedentes de los usuarios. • Implementar el registro de las actividades realizadas (Pistas de auditoría). • Mantener responsabilidad sobre cada acción impidiendo que se compartan cuentas.
4	Listas de Acceso.	Las entidades implementarán listas de acceso que discriminen el tráfico de red.
		Las entidades implementarán procedimientos de gestión de cambios en el que se

5	Gestión de cambios	introduzcan las autorizaciones, ajustes y variaciones que se realicen en la Entidad de una manera ordenada y controlada.
6	Gestión de Parches y versionamiento.	Las entidades implementarán procedimientos de gestión de parches y versionamiento a través de los cuales se actualicen a las últimas versiones estables recomendadas por los diferentes fabricantes y proveedores.
7	Gestión de la configuración.	Las entidades implementarán procedimientos para la gestión de configuraciones del activo tecnológico como son dispositivos de red, sistemas, aplicaciones, canales electrónicos, servicios propios y/o proporcionados por terceros entre otros.
8	Generar y establecer simulaciones de posibles ataques. (Pruebas de penetración).	Las entidades deberán al menos una vez al año revisar la seguridad de sus activos mediante ejercicios prácticos y controlados, que simulen varios tipos de amenazas posibles, tales como ethical hacking, pentesting, entre otros; exponiendo a la infraestructura que soporta los servicios de la Entidad a diferentes escenarios de nivel básico a avanzando en medida de lo posible.
9	Implementar la arquitectura de seguridad la entidad.	Las entidades deberán implementar una arquitectura de seguridad en la que se considere políticas, procesos, procedimientos e infraestructura de tecnología interna y/o de terceros que garanticen la gestión de amenazas y ataques que permita obtener indicadores de compromiso a través del análisis contextual y de comportamiento, escaneo de vulnerabilidades, análisis de riesgos de terceros, simulación de adversarios, ingeniería social, con controles

		de red, prevención de fuga de información, gestión de parches, denegación de servicios y estándares de cifrado, entre otros.

Los aspectos tratados en el presente, deberán ser tomados como recomendaciones que aportarán en el manejo de la información y administración de la ciberseguridad en las entidades como un punto de apoyo para la mejora continua a sus procesos de seguridad interna.

---

[1] Usuarios, tecnología y normativa

Atentamente,

Firmado electrónicamente por:
Catalina Pazos Chimbo
INTENDENTE GENERAL TÉCNICO
2021-08-23 19:33:34

Catalina Pazos Chimbo
INTENDENTE GENERAL TÉCNICO