PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN AÑO 2019

Enero 2019

INTRODUCCIÓN

Teniendo en cuenta La Política de Gobierno Digital como un componente del Modelo Integrado de Planeación y Gestión MIPG, la entidad acogiendo los lineamientos y mejores prácticas establecidas en diferente Normatividad, para la Vigencia 2019 realizará las actividades descritas en el presente plan, el cual forma parte integral del Plan de Gestión Institucional de Prosperidad Social.

OBJETIVO

Definir el plan de Tratamiento de Riesgos de seguridad de la información para el año 2019, el cual forma parte integral del Plan de Gestión Institucional de Prosperidad Social, para preservar los criterios de confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información en Prosperidad Social.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1.1 Amenazas con mayor probabilidad de ocurrencia

Al realizar un proceso de filtrado de la matriz de riesgos del SGSI y seleccionando las amenazas con mayor probabilidad de ocurrencia se identifican las siguientes:

- Abuso de privilegios en el uso de activos de información (equipos, sistemas de información, documentos, servicios de información)
- Brechas en disponibilidad de personal (ausencia e insuficiencia de personal necesario para cumplir con las actividades de los procesos)
- Copia fraudulenta de datos (copia o extracción de información de las bases de datos de Prosperidad Social)
- Corrupción de datos (alteración de los datos almacenados en sistemas de información de manera intencional o por error)
- Ingreso sin autorización a las áreas físicas
- Error en el uso de equipos (por ausencia de procedimientos documentados)
- Fallas en suministro de energía eléctrica por insuficiencia en la capacidad de la UPS
- Ingeniería social (Falta de conciencia y deficiencia en la formación y sensibilización en seguridad de la información)
- Pérdida de datos (por ausencia de comprobación de copias de respaldo)
- Revelación de información (Debilidad en los controles para la clasificación de información)

- Denegación de servicios (pérdida de la disponibilidad de servicios por saturación del sistema o por ataque informático)

1.2 Vulnerabilidades con mayor probabilidad de ocurrencia

Al realizar el proceso de filtrado de la matriz de riesgos del SGSI y seleccionando las vulnerabilidades más frecuentes identificadas se encontró:

- Falta de conciencia en seguridad de la información
- Debilidad en los controles para copias de respaldo de información almacenada en estaciones de trabajo
- Debilidad en la documentación de procedimientos de operación
- Ausencia de mecanismos de monitoreo de personal
- Ausencia de registros de auditoría
- Ausencia de procedimientos formales para supervisar el procesamiento de información
- Debilidad en los controles para clasificación de información
- Ausencia de procedimientos para revisión de registros de auditoría
- Deficiencia en los controles de autorización de acceso.
- Insuficiencia en los controles de carpetas compartidas (sin contraseña y con control total)
- Conexiones a redes públicas desprotegidas
- Copias de datos no controladas
- Deficiente o insuficiente entrenamiento en seguridad de la información
- Falta de control en la configuración o hardening de equipos
- Incorrecta asignación de privilegios
- Logs (registros de auditoría) incompletos
- No se escolta a los visitantes durante la permanencia en las sedes de la entidad
- Insuficiencia en la documentación para le gestión de la capacidad
- Insuficiencia en el análisis de vulnerabilidades
- Deficiencia en el cifrado de la información
- Planes de continuidad desactualizados
- Reúso de medios sin procedimiento de borrado seguro
- Tráfico de datos sensibles no protegido

- Uso deficiente de controles de acceso a sedes
- Vulnerabilidades técnicas de bases de datos
- Vulnerabilidades técnicas de sistema operacional

Teniendo en cuenta el Mapa de Riesgos institucional específicamente en los riesgos relacionados con la seguridad de la Información, se seleccionan los controles para mitigar los riesgos inherentes a los 114 controles propuestos por la norma ISO 27001:2013.

De otra parte y con el fin de dar cumplimiento a los objetivos del SGSI, es necesario realizar las siguientes actividades teniendo en cuenta que algunas de ellas están en etapa de implementación y/o se deben implementar:

Controles Seleccionados	**Descripción de actividades**
6.1.8 Se realiza Auditoría interna	Programar una auditoria interna al SGSI alineada a la norma ISO19011
6.1.6 Contacto con las autoridades	Establecer grupos de interés y definir puntos de contacto
7.1.1 Inventario de activos tecnológicos y de la información. 7.1.2 Responsables de los activos tecnológicos	Revisar el cumplimiento de la metodología para la gestión de activos. Implementar un mecanismo para la actualización del inventario de activos de información.
7.1.3 Uso aceptable de los activos tecnológicos	Llevar a cabo campañas mensuales para sensibilizar a los funcionarios sobre la aplicación de la política de uso aceptable de recursos tecnológicos de la entidad.
7.2.1 Normas para clasificación de la información 7.2.2 Identificación y Manejo de la información	Evaluar la aplicación de la guía de clasificación de información que contempla niveles de sensibilidad distintos e indica el tratamiento que debe tener la información de acuerdo con su criticidad.
8.2.3 Procesos disciplinarios	Implementar la política y/o procedimiento para los procesos disciplinarios asociados a incidentes de seguridad
8.3.2 Devolución de activos tecnológicos 9.2.6 Eliminación, destrucción y reutilización de equipos	Implementar la política de borrado seguro y de devolución de activos..

9.1.2 Controles físicos de entrada 9.1.3 Aseguramiento de oficinas, cuartos e instalaciones 9.1.5 Trabajo en áreas restringidas / seguras 9.1.6 Acceso público, envíos y áreas de carga	Evaluar la eficiencia de las puertas de control de acceso y el procedimiento de ingreso de invitados/visitantes. Establecer cultura organizacional, para fomentar el uso del carnet de los colaboradores de la entidad. Revisar la seguridad física de los servidores y las estaciones críticas de trabajo. Validar la instalación de cámaras de seguridad en el área de procesamiento de datos.
9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	Revisar la seguridad física de los servidores y las estaciones de trabajo. Validar la instalación de cámaras de seguridad.
9.1.4 Protección contra amenazas externas y ambientales	Revisar el funcionamiento y gestión del sistema de aire acondicionado y sistema de detección y extinción de fuego.
9.2.1 Ubicación y protección de equipos tecnológicos	Revisar la seguridad física de los servidores y las estaciones de trabajo. Validar la instalación de cámaras de seguridad.
9.2.4 Mantenimiento de los equipos	Definir un plan de mantenimiento para los componentes físicos de infraestructura donde se establezca periodicidad del mantenimiento correctivo en función del tipo de activo. La ejecución de las actividades de mantenimiento puede estar a cargo de un tercero o un funcionario para lo cual se debe hacer una definición de roles y funciones.
10.10.1 Registros de Auditoría	Implementar la política de auditoria que defina de acuerdo a los niveles de sensibilidad para cada activo, la frecuencia de revisión, el alcance de cada auditoria a sistemas de información y el periodo de retención.
10.10.2 Monitoreo del uso del sistema	Implementar la política que estipule las condiciones sobre las cuales se deba hacer el monitoreo al uso de sistemas, sin violar la privacidad de los usuarios, pero garantizando el seguimiento a actividades propias de la organización.

10.10.3 Protección de registros de monitoreo	Implementar dentro de la política de monitoreo las condiciones de almacenamiento y custodia que deben tener los registros de monitoreo.
10.10.4 Registros de monitoreo de administradores y operadores	Implementar la política que estipule las condiciones sobre las cuales se deba hacer el monitoreo al uso de sistemas por parte de administradores y operadores garantizando el seguimiento a actividades propias de la organización.
10.8.3 Medios físicos en tránsito	Validar el cumplimiento de la política para el transporte de información en medios físicos.
10.10.5 Registro de fallas	Revisar la efectividad del sistema de registro y almacenamiento de fallas para los activos de información. Validar la creación de la base de datos de conocimiento (KDB)
10.5.1 Respaldo de la información.	Evaluar el cumplimiento de la política de Back up para la información. Revisar la actualización de las tablas de retención documental.
10.7.4 Seguridad de la documentación de los sistemas intercambio de información.	Validar que los sistemas de información cuenten con los manuales y que la documentación asociada a los mismos sea accesible por las personas que la requieren sin revelarla a personas no autorizadas.
10.9.3 Información pública / disponible al público	Registrar la revisión del procedimiento de publicación de información o puesta en producción de nuevos módulos, para garantizar la veracidad de la información.
10.8.5 Sistemas de información de la entidad	Implementar política para la conexión segura a sistemas de información de la entidad: Perfiles de acceso, clasificación de información, acceso a información sensible, identificación y mitigación de vulnerabilidades conocidas. Validar la ejecución segura de programas autorizados por medio de HIPS, APP control y Firewall para servidores, según el caso.
10.3.2 Aceptación de sistemas	Implementar la política de aceptación de sistemas de información, que incluye entre otros: documentación asociadas, pruebas de seguridad, fiabilidad de la arquitectura, entre otros.
10.7.1 Gestión de medios removibles	Evaluar el cumplimiento de la política de gestión de medios removibles que determine las

	condiciones y la forma como se permitirá la utilización de dispositivos extraíbles. Esto implica la adopción de cifrado en medios removibles por lo cual se deberá validar la adquisición de una herramienta para cifrado robusto en medios removibles.
10.7.2 Destrucción de medios	Implementar la política de borrado seguro que defina el procedimiento, herramientas y mecanismos de verificación aplicables para casos de destrucción de medios.
10.1.2 Contra de cambios	Implementar la política de gestión de cambios.
10.3.1 Gestión de la capacidad	Implementar la política de gestión de capacidad.
11.7.2 Teletrabajo / trabajo remoto	Verificar la aplicación de la política y procedimiento de gestión de cambios y trabajo remoto.
11.1.1 Política de Control de Acceso	Revisar que en las aplicaciones y en los sistemas de información se encuentre implementada la política de control de acceso lógico, que determine los requisitos para la autorización de permisos, la segregación de perfiles en cada caso, la separación de funciones (SoD), los periodos de revisión de permisos, entre otros.
11.2.1 Registro de Usuarios y Gestión de privilegios	Validar el cumplimiento del procedimiento para la asignación y revocación de privilegios se usuario, al igual que los registros para cada operación de administración. Revisar que, cada vez que se retira o desvincula de la entidad una persona, se le debe desactivar las cuentas que tenía asignadas. En el sistema de control biométrico es posible que existan usuarios habilitados, de personas que ya no trabajan en la entidad. Se debe hacer un chequeo en profundidad del tema, para depurar UsersIDs que ya no se requieren en éste y en los demás sistemas. Hacer una comparación exhaustiva en cada uno de los componentes de sistemas (Aplicaciones y Dominio), para depurar y borrar aquellos usuarios que ya no laboran en la entidad.

	Verificar que, en los aplicativos y sistemas de información, se bloquee después del sexto o menos intentos fallidos de acceso. Y permanezca bloqueada por un tiempo determinado o hasta que un rol administrador la desbloquee.
11.2.3 Gestión y uso de Contraseñas (passwords)	Validar que en las aplicaciones y sistemas de información se estipulen los requisitos mínimos para la creación, transmisión y cambio de contraseñas. sensibilizar a usuarios y administradores sobre la aplicación de esta política.
11.4.2 Autenticación de usuarios para conexiones externas	Revisar el cumplimiento de la política para el uso de conexiones seguras alternas: VPN. Evaluar la posibilidad de tener múltiples factores de autenticación.
11.5.2 Identificación y autenticación de los usuarios.	Fortalecer el proceso de autenticación de usuarios con factores de autenticación robustos. Evaluar uso de OTP.
11.4.1 Políticas para el uso de los servicios de la red de datos	Verificar el cumplimiento de la política de uso aceptable de activos, los aspectos relacionados a uso de la red
11.4.3 Identificación de equipos en la red	Definir mecanismos para la identificación de equipos corporativos y externos en la red. Aplicar a cada uno un tratamiento diferente de acuerdo a las necesidades.
11.4.4 Diagnóstico remoto y protección de la configuración de puertos	Validar la apertura de los puertos que son estrictamente necesarios para el funcionamiento de los sistemas de información.
11.4.5 Separación en la red	Revisar y auditar la segregación de redes actual.
11.4.6 Control de conexión a la red de trabajo	Definir mecanismos para la identificación de equipos corporativos y externos en la red. Aplicar a cada uno un tratamiento diferente de acuerdo a las necesidades.
11.4.7 Control de enrutamiento de red	Validar las políticas de enrutamiento actuales a la luz de las buenas prácticas de seguridad.

12.5.3 Restricciones a cambios en paquetes de software	Implementar la política y procedimiento de gestión de cambios
12.6.1 Control técnico de vulnerabilidades	Revisar semestralmente las vulnerabilidades técnicas conocidas, valorarlas de acuerdo a la metodología de riesgos (Risk Advisor) y tratarlas con prioridad de acuerdo a criticidad del activo. Hacer escaneo de vulnerabilidades que incluyan pruebas de intrusión (OpenVAS, Vulnearbility Manager)
12.4.1 Control del software operacional(operativo)	Implementar la política y procedimiento de gestión de cambios.
12.5.1 Procedimientos para el control de cambios	Implementar la política y procedimiento de gestión de cambios.
12.5.2 Revisión técnica de aplicaciones después de cambios al sistema operativo	Implementar la política y procedimiento de gestión de cambios que incluya revisión de cambios aplicados, plan de roll back, plan de contingencia, entre otros.
12.2.1 Validación de los datos de entrada	Efectuar la validación de parámetros de entrada a aplicativos desde una perspectiva ofensiva utilizando buenas prácticas para revisión de software (OWASP)
12.2.2 Control del procesamiento interno	Definir mecanismos de validación de integridad utilizando HASH, Checksum o algún mecanismo fiable.
12.2.3 Integridad de los mensajes	Definir mecanismos de validación de integridad utilizando HASH, Checksum o algún mecanismo fiable.
12.2.4 Validación de los datos de salida	Definir directrices para la prueba de salidas de sistemas de acuerdo a OWASP.
12.3.1 Política para el uso de controles criptográficos	Validar la aplicación de la política de cifrado que dé cumplimiento a la legislación aplicable, mediante la utilización de protocolos como SSL/TLS, IPSEC, SSH, entre otros.
12.3.2 Gestión de llaves	Implementar la política para la gestión de llaves: generación, distribución, revocación y demás.
15.2.2 Verificación del cumplimiento técnico	Auditar el cumplimiento del manual de políticas de seguridad de la información.