SEGURIDAD Y CONTINUIDAD SETI

SETI se encuentra en proceso de certificación en ISO27001 y cuenta con un avance en la implementación de los controles descritos en el anexo A de la norma del 96%. La organización tiene como meta lograr el 100% de implementación de los controles de seguridad y obtener la certificación ISO27001 antes de finalizar el año 2022.

En la Política de Seguridad de la Información se definen los lineamientos para el tratamiento de Seguridad de la Información por parte de la Gerencia de Tecnología y el área de Seguridad. Igualmente da orientaciones con respecto de los recursos como Internet, Computadores, Correo electrónico entre otros, por parte de los colaboradores de SETI y se definen los controles tecnológicos aplicados al interior de la organización con los cuales se garantiza la integridad, disponibilidad y confidencialidad de la información. Algunos de estos controles son:

- Directorio Activo para la creación de cuentas de usuario, aplicación de políticas en los computadores y asignación de permisos de acceso a recursos.
- Software antivirus licenciado e instalado en todos los equipos y administrados mediante una consola central la cual permite monitorear eventos y realizar revisiones de las versiones y actualizaciones instaladas. Este antivirus adicionalmente cuenta con los módulos de Web Control y DLP configurados de acuerdo con las necesidades.
- Seguridad perimetral de la red para proteger la infraestructura con dispositivos Fortigate que incluyen firewall, antivirus e IPS, además de control de acceso a sitios web potencialmente peligrosos desde las oficinas de SETI.
- Protección WAF y certificados TLS para aplicaciones expuestas a internet.
- Conexión VPN con MFA para los integrantes que accedan a información de forma remota.
- Políticas de contraseñas seguras.

- Se realizan análisis de hacking ético con un proveedor externo anualmente, con el fin de identificar y cerrar vulnerabilidades en los sistemas.

Los privilegios de los integrantes de SETI son solicitados por los lideres, inicialmente, antes del ingreso. Para esto se diligencia la lista de chequeo, la cual es entregada a Talento Humando, donde se indican los que permisos necesarios, acceso a aplicaciones, VPNs, o privilegios especiales que necesita el integrante para desempeñar sus actividades.

En caso de ser necesarios privilegios adicionales después de la vinculación del integrante, estos deberán ser tramitados por medio de la herramienta de gestión de solicitudes (GLPI) únicamente por el gerente o líder del proyecto.

Los permisos y accesos que los integrantes de SETI necesiten para desarrollar actividades sobre los sistemas de los clientes, serán suministrados y administrados por los clientes.

SETI cuenta con políticas que aseguran una adecuada gestión de las cuentas de usuario privilegiado, con el fin de prevenir riesgos asociados por el uso inadecuado de estos privilegios. La compañía define las cuentas de usuario privilegiado sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones, el Gerente del servicio será el responsable de suministrar los accesos a esta información a los integrantes de los diferentes equipos de soporte.

Dentro de nuestro proceso de selección incluimos estudio de seguridad, el cual se incluye validación de referencias laborales, estudio, personas, visita domiciliaria, validaciones centrales de riesgo y procesos judiciales. Antes de iniciar este proceso los candidatos firman autorización Informada y tratamiento de datos personales de acuerdo con la ley 1581 de 2012

SETI ha identificado y clasificado los activos de información de acuerdo con su confidencialidad, lo que permite identificar los riesgos y tomar las acciones necesarias para prevenir la fuga de información. Además, se cuenta con la herramienta de DLP de Trellix (McAfee) instalada en los equipos SETI la cual restringe el copiado de información a dispositivos USB externos. Todos nuestros consultores firman acuerdos de confidencialidad al momento de la firma del contrato.

Se cuenta con un normograma alineada bajo los estándares de la ISO 27001 y con lineamientos de las C.E 042 y 007, las cuales se adoptan por requerimientos de nuestros clientes, pero que no son de obligatorio cumplimiento.

Para la continuidad del negocio SETI se implementan buenas prácticas basadas en la norma ISO31000 donde se plantea la contingencia de la infraestructura tecnológica, personas y procesos. Estas políticas se encuentran en el documento Plan de Continuidad del Negocio. También se cuenta con el plan de comunicación de crisis y el plan de Gestión de incidentes, documentos que dan los lineamientos para la atención de situaciones críticas al interior de la organización. Adicionalmente se tiene los lineamientos en torno a la ejecución de pruebas de continuidad de internet, y pruebas de restauración de servicio con las que se validan la integridad y la disponibilidad de la información.

La gestión de riesgos es estándar y transversal en la compañía, los riesgos se manejan tanto en la estrategia como la operación y se dispone de una Matriz de Riesgos y Controles específica por cada proyecto y por cada proceso gestionada a través de la plataforma GPS, con revisiones y actualizaciones periódicas.

Como mecanismo para garantizar el cumplimiento de las políticas y programas de la compañía, se llevan cabo revisiones periódicas de la oficina de Gobierno Corporativo de la compañía, teniendo como insumos los resultados de las auditorías internas y las auditorías externas que adelantan los diferentes clientes en sus procesos de control de proveedores. Todos estos resultados, son escalados al comité de buenas prácticas de SETI, donde participa la alta dirección y se consolida el proceso de control y seguimiento.